are now embedded in products and in the entire technology stack. The question is, who should be responsible for this new technology infrastructure: IT, R&D, or some combination of both?

Only IT currently has the skills to support the software-based technologies and related infrastructure that smart, connected products require. R&D organizations, for their part, have been good at developing and combining mechanical and electrical components, and many have begun to master the challenge of incorporating software in products. Few R&D organizations, however, have deep experience in building and managing the cloud-based elements of the technology stack. Now, IT and R&D must integrate their activities on a continual basis. Yet the two functions have little history of collaboration on product development—and in some organizations have a history of animosity.

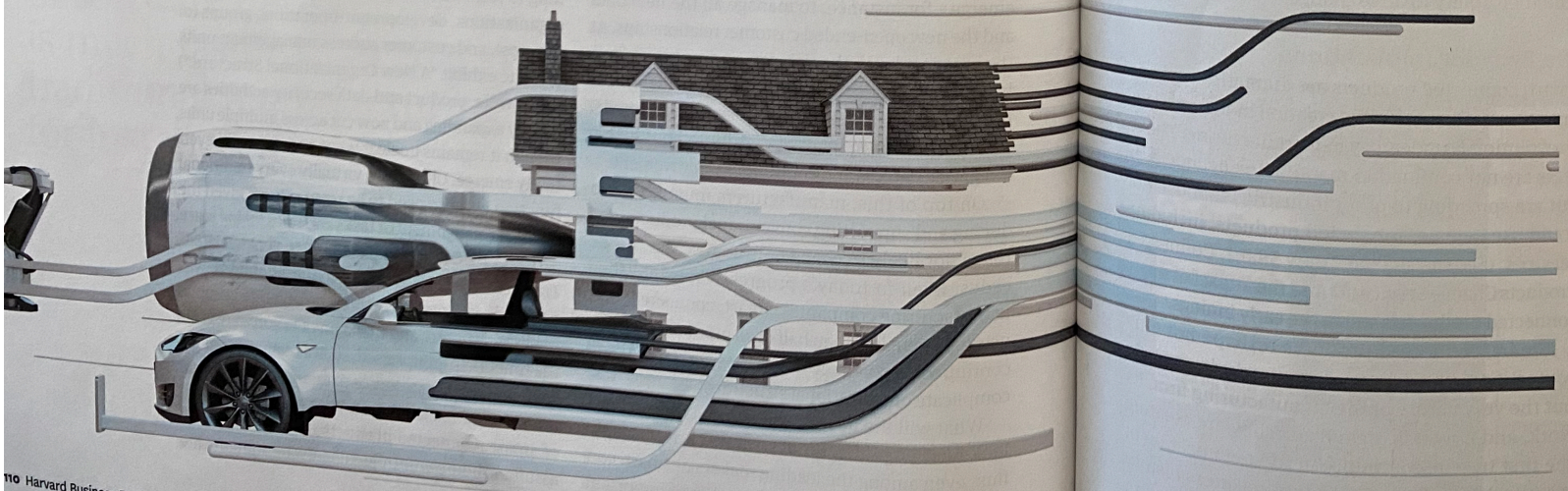
Various organizational models for this new relationship are emerging. Some companies are embedding IT teams within R&D departments. Others are establishing cross-functional product design teams that include IT representation while maintaining separate reporting lines. For example, at Ventana Medical Systems, a maker of smart, connected lab equipment, the IT and R&D teams now work jointly on product development, with IT weighing in heavily on choices about what product functionality should be delivered in the cloud and when software updates are needed. At Thermo Fisher Scientific, a scientific instrument leader, members of the IT department work directly inside R&D, with a dotted-line reporting structure and shared goals. This has improved Thermo Fisher's effectiveness at defining and building the product cloud; securely capturing, analyzing, and storing product data; and distributing data both internally and to customers.

A UNIFIED DATA ORGANIZATION. Because of the growing volume, complexity, and strategic importance of data, it is no longer desirable or even feasible for each function to manage data by itself, build its own data analytics capability, or handle its own data security. To get the most out of the new data resources, many companies are creating dedicated data groups that consolidate data collection, aggregation, and analytics, and are responsible for making data and insights available across functions and business units. The research firm Gartner predicts that by 2017 as many as a quarter of all large firms will have dedicated data units.

The new data organizations usually are led by a C-level executive, the chief data officer, who reports to the CEO or sometimes to the CFO or CIO. He or she is responsible for unified data management, educating the organization on how to apply data resources, overseeing data rights and access, and driving the application of advanced data analytics across the value chain. Ford Motor Company, for example, recently appointed a chief data and analytics officer to develop and execute an enterprise-wide vision for data analysis. The CDO is spearheading the company's use of smart, connected product data to understand customer preferences, shape future strategies for connected cars, and restructure internal processes.

DEV-OPS. The imperatives of evergreen product design, continuous product operation and support, and ongoing product upgrades are creating a need for a new functional group, sometimes called dev-ops. (The term comes from the software industry, where it is used to describe a collaborative, cross-functional software development and deployment method.) The dev-ops unit is responsible for managing and optimizing the ongoing performance of connected products after they have left the factory. It brings together software-engineering experts from the traditional product-development organization (the "dev") with staff members from IT, manufacturing, and service who are responsible for product operation (the "ops").

Dev-ops organizes and leads teams that shorten product-release cycles, manage product updates and patches, and deliver new services and enhancements postsale. It oversees the frequent release of small, carefully tested batches of product changes into the shared cloud, ideally with no disruption to existing products and users in the field. The dev-ops organization also leads the work to enhance preventive service models and product maintenance.



CUSTOMER SUCCESS MANAGEMENT. A third new organizational unit, which also has an analogue in the software industry, is responsible for managing the customer experience and ensuring that customers get the most from the product. This task is crucial with smart, connected products, especially to ensure renewals in product-as-a-service models. The customer success management unit does not necessarily replace sales or service units but assumes primary responsibility for customer relationships after the sale. This unit performs roles that traditional sales and service organizations are not equipped for and don't have incentives to adopt: monitoring product use and performance data to gauge the value customers capture and identifying ways to increase it. This new unit does not operate as a self-contained silo but collaborates on an ongoing basis with marketing, sales, and service.

Customer success units are changing the management of customer relationships. Historically, customer surveys and call centers have been the principal ways companies gather insights about product use and determine when a customer relationship is in jeopardy. Companies typically hear most from customers when something goes wrong—and often not until it is too late.

With smart, connected products, the product itself becomes a sensor that gauges the value customers are receiving. Through the data it generates, a product can tell companies a lot about the customer experience: about product use and performance, customer preferences, and customer satisfaction. Such insights can prevent customer defections and reveal where a customer could benefit from additional product capabilities or services.

SHARED RESPONSIBILITY FOR SECURITY. In most companies, executive oversight of security is in flux. Security may report to the chief information officer, the chief technology officer, the chief data officer, or the chief compliance officer. Whatever the leadership structure, security cuts across product development, dev-ops, IT, the field service group, and other units. Especially strong collaboration among R&D, IT, and the data organization is essential. The data organization, along with IT, will normally be responsible for securing product data, defining user access and rights protocols, and identifying and complying with regulations. The R&D and dev-ops teams will take the lead on reducing vulnerabilities in the physical product. IT and R&D