

equipment made by Sysmex is a good example. Sysmex originally added connectivity to its instruments to allow remote monitoring but now uses it to provide service as well. Service technicians can access just as much information about a machine when they are off-site as when they are on-site. Often they can fix it by rebooting it, delivering a software upgrade, or talking an on-site medical technician through the process. As a result, service costs, equipment downtime, and customer satisfaction have improved dramatically.

Preventive service. Using predictive analytics, organizations can anticipate problems in smart, connected products and take action. Diebold, for example, monitors its automated teller machines for early signs of trouble. It performs the necessary maintenance remotely, if possible, or dispatches a technician to adjust or replace parts. The company can also update a machine with preventive fixes when feature enhancements are added, sometimes remotely.

The job of ensuring IT security now cuts across all functions. Every smart, connected device may be a point of network access or a target of hackers.

Augmented-reality-supported service. The vast amounts of data that smart, connected products gather are creating new ways for service personnel to work individually, together, and with customers. One emerging approach utilizes the augmented reality overlays we described earlier. When these include information about a product's service needs and step-by-step repair instructions, service efficiency and effectiveness can increase dramatically.

New services. The data, connectivity, and analytics available through smart, connected products are expanding the traditional role of the service function and creating new offerings. Indeed, the service organization has become a major source of business innovation in manufacturing, driving increased revenue and profit through new value-added services such as extended warranties and comparative benchmarking

across a customer's equipment, fleet, or industry. The array of solutions that Caterpillar has developed to help customers manage its construction and mining equipment is a good example. After gathering and analyzing data for each machine deployed at a work site, Caterpillar's service teams advise customers on where to locate equipment, when fewer machines could suffice, when to add new equipment to reduce bottlenecks, and how to achieve higher fuel efficiency throughout a fleet.

SECURITY. Until recently, IT departments in manufacturing companies have been largely responsible for safeguarding firms' data centers, business systems, computers, and networks. With the advent of smart, connected devices, the game changes dramatically. The job of ensuring IT security now cuts across all functions.

Every smart, connected device may be a point of network access, a target of hackers, or a launchpad for cyberattacks. Smart, connected products are widely distributed, exposed, and hard to protect with physical measures. Because the products themselves often have limited processing power, they cannot support modern security hardware and software.

Smart, connected products share some familiar vulnerabilities with IT in general. For example, they are susceptible to the same type of denial-of-service attack that overwhelms servers and networks with a flood of access requests. However, these products have major new points of vulnerability, and the impact of intrusions can be more severe. Hackers can take control of a product or tap into the sensitive data that moves between it, the manufacturer, and the customer. On the TV program *60 Minutes*, DARPA demonstrated how a hacker could gain complete control of a car's acceleration and braking, for example. The risk posed by hackers penetrating aircraft, automobiles, medical equipment, generators, and other connected products could be far greater than the risks from a breach of a business e-mail server.

Customers expect products and their data to be safe. So a firm's ability to provide security is becoming a key source of value—and a potential differentiator. Customers with extraordinary security needs, such as the military and defense organizations, may demand special services.

Security will affect multiple functions. Clearly the IT function will continue to play a central role in identifying and implementing best practices for data and network security. And the need to embed

security in product design is crucial. Risk models must consider threats across all potential points of access: the device, the network to which it is connected, and the product cloud. New risk-mitigation techniques are emerging: The U.S. Food and Drug Administration, for example, has mandated that layered authentication levels and timed usage sessions be built into all medical devices to minimize the risk to patients. Security can also be enhanced by giving customers or users the ability to control when data is transmitted to the cloud and what type of data the manufacturer can collect. Overall, knowledge and best practices for security in a smart, connected world are rapidly evolving.

Data privacy and the fair exchange of value for data are also increasingly important to customers. Creating data policies and communicating them to customers is becoming a central concern of legal, marketing, sales and service, and other departments. In addition to addressing customers' privacy concerns, data policies must reflect ever-stricter government regulations and transparently define the type of data collected and how it will be used internally and by third parties.

HUMAN RESOURCES. A manufacturer of smart, connected products is a cross between a software company and a traditional product company. This mix demands new skills across the value chain, as well as new working styles and cultural norms.

New expertise. The skills needed to design, sell, and service smart, connected products are in high demand but short supply. Indeed, manufacturers are experiencing a growing sense of urgency about finding the right talent as their skill requirements shift from mechanical engineering to software engineering, from selling products to selling services, and from repairing products to managing product uptime.

Manufacturers will have to hire experts in applications engineering, user interface development, and systems integration, and, most notably, data scientists capable of building and running the automated analytics that help translate data into action. The business or data analyst of the past is evolving into a new type of professional, who must possess both technical and business acumen as well as the ability to communicate insights from analytics to business and IT leaders.

The shortage of these new skills is especially acute in traditional manufacturing centers, many of which are different from technology hubs. So some

LESSONS FROM THE SOFTWARE INDUSTRY

Many of the organizational shifts that smart, connected products are bringing to manufacturing mirror changes that have already taken root in the software industry. This is not surprising, since the evolution to smart, connected products requires a traditional manufacturer to build what is essentially an internal software company.

The software industry, with an entirely digital product, was early to deploy its products both on premise and in the cloud and to support them remotely. Software companies also were in the forefront in improving products continuously, including after the sale.

The organizational lessons that other industries can draw from software fall into five categories:

- 1 SHORTER DEVELOPMENT CYCLES:** The software industry has moved away from periodic releases of major products to smaller, incremental releases of upgrades and enhancements. Because of this, companies can get new products to market more quickly and respond faster to customer needs. Agile product-development processes—which emphasize daily collaboration between developers and marketers, weekly delivery of enhancements, continual course corrections, and ongoing testing of customer satisfaction—are best practice in software development.
- 2 PRODUCT-AS-A-SERVICE BUSINESS MODELS:** Software is undergoing a sectorwide transition to service-oriented business models. Customers purchase software on a subscription basis, paying only for what they need when they need it, instead of buying "shelfware" that sits idle. This turns the product into an operating, rather than capital, expense, and hugely simplifies deployment (which happens via the cloud). To support this new model, software companies have learned to carefully track customer usage and satisfaction.
- 3 FOCUS ON CUSTOMER SUCCESS:** The shift toward software-as-a-service models has led to the rise of customer success organizations inside software companies. Given the ease with which customers can change vendors, ensuring that they receive superior ongoing value from products is critical. Many software companies now have customer engagement teams dedicated to pursuing that goal.
- 4 PRODUCTS PART OF BROADER SYSTEMS:** Most software is deployed as part of a larger "stack" of business tools, whose value is enhanced by their integration. Successful software companies often provide application program interfaces and other tools that enable easy integration of their product with third-party software. In addition, software companies often encourage the formation of developer communities to create new uses for their products.
- 5 ANALYTICS AS A COMPETITIVE ADVANTAGE:** Software companies, especially those in e-commerce, have long understood the power of data analytics in generating customer value. Companies with an advertising revenue model use analytics to serve up ads at the right time—when customers are most likely to notice and act on them. Increasingly, software companies are also mining data on use to identify bugs with the highest impact on customers.

manufacturers are establishing a physical presence in hot spots such as Boston and Silicon Valley, which combine a presence in advanced manufacturing with academic centers, makers of B2B hardware and software, and emerging producers of smart, connected products. Schneider Electric, for example, is moving its U.S. headquarters to Boston. Over the next decade, manufacturers can accelerate their learning and improve recruiting by being in such clusters. But they will also need new recruiting models, like