BCG

The Boston Consulting Group

APRIL 2017

BCG TECHNOLOGY ADVANTAGE

- Looking into the Future of Artificial Intelligence
- Five Lessons from B2C Leaders on Digital Transformation
- Digital Transformation: From Black Box to Crystal Clear
- Winning in IoT: It's All About the Business Processes
- Leaner, Faster, and Better with DevOps
- Building a Cyberresilient Organization
- Report from Davos: Board Oversight of Cyberresilience

Competing in the Age of Artificial Intelligence

The Boston Consulting Group (BCG) is a global management consulting firm and the world's leading advisor on business strategy. We partner with clients from the private, public, and not-for-profit sectors in all regions to identify their highest-value opportunities, address their most critical challenges, and transform their enterprises. Our customized approach combines deep insight into the dynamics of companies and markets with close collaboration at all levels of the client organization. This ensures that our clients achieve sustainable competitive advantage, build more capable organizations, and secure lasting results. Founded in 1963, BCG is a private company with 85 offices in 48 countries. For more information, please visit bcg.com.

Preface

"Man versus machine." The concept has fueled many stories about the possibilities and challenges that technology poses. Given the inexorable wave of digital disruption, it's time to turn stories into strategies.

Much of the digital change today is powered by artificial intelligence (AI), primarily machine learning (ML). AI and ML will become foundational technologies in the digital world. As man taps the power of these machines, leaders will confront a number of important and difficult questions involving job elimination and job creation, distribution of the wealth created by digital, and other issues that carry serious ethical and moral ramifications.

Leaders might find that in a digital, AI-enabled world, their "EQ" (emotional or ethical intelligence) matters as much or more than their IQ when it comes to seeking out answers to those important questions and establishing strategies to guide their enterprises through organizational change and new ways of working. Linking EQ, IQ, and "AIQ" is a powerful formula for a new and transformational leadership solution.

Amid profound digital transformation, how do leaders replace the concept of "man *versus* machine" with one of "machine-*enabled* man," and how do they bring that new paradigm to life? In this edition of *BCG Technology Advantage,* we explore this complex topic from a variety of perspectives:

- What to consider now as an enterprise competing in the age of AI and what to anticipate in the future
- How B2C businesses can make the most of digital transformation
- Why changes to business processes and IT development operations can improve an organization's outcomes, and how to implement those changes
- Why cyberresilience is critical and how to establish it

We hope that you find these articles interesting and thought provoking—and we hope that you will share your thoughts with us at Technology.Advantage@bcg.com.

Ralf Dreischmeier
Global Leader, Technology Advantage practice

Contents

COMPETING IN THE AGE OF ARTIFICIAL INTELLIGENCE

by Philipp Gerbert, Jan Justus, and Martin Hecker

Until recently, artificial intelligence (AI) was similar to nuclear fusion in unfulfilled promise. It had been around a long time but had not reached the spectacular heights foreseen in its infancy. Now, however, AI is realizing its potential in achieving human-like capabilities, so it is time to ask: How can business leaders harness AI to take advantage of the specific strengths of man and machine?

AI is swiftly becoming the foundational technology in areas as diverse as self-driving cars and financial trading. Self- learning algorithms are now routinely embedded in mobile and online services. Researchers have leveraged massive gains in processing power and the data streaming from digital devices and connected sensors to improve AI performance. And machines have essentially cracked speech and vision specifically and human communication generally. The implications are profound:

- Because they know how to speak, read text, and absorb and retain encyclopedic knowledge, machines can interact with people intuitively and naturally on a wide range of topics at considerable depth.

- Because they can identify objects and recognize optical patterns, machines can leave the virtual and join the real world.

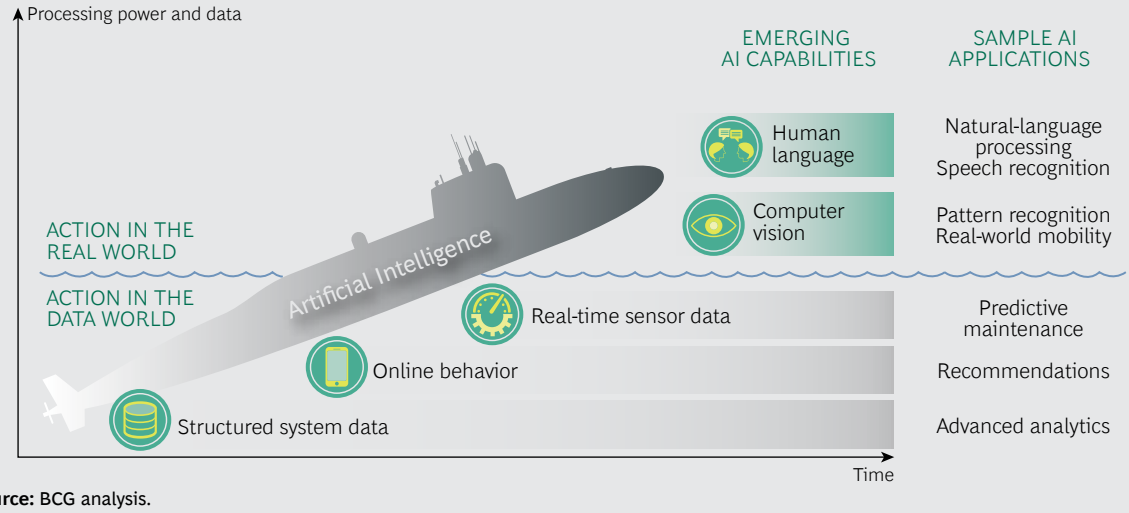
A field that once disappointed its proponents is now striking remarkably close to home as it expands into activities commonly performed by humans. (See Exhibit 1 and the sidebar.) AI programs, for example, have diagnosed specific cancers more accurately than radiologists. No wonder that traditional companies in finance, retail, health care, and other industries have started to pour billions of dollars into the field.

Traditional companies have started to pour billions of dollars into the AI field.

Because AI systems think and interact, they are invariably compared to people. But while humans are fast at parallel processing (pattern recognition) and slow at sequential processing (logical reasoning), computers have mastered the former in narrow fields and are superfast in the latter. Just as submarines don't swim, machines solve problems and accomplish tasks in their own way.

Without further quantum leaps in processing power, machines will not reach artificial general intelligence (AGI): the combination of vastly different types of problem-solving ca-

EXHIBIT 1 | By Cracking Language and Vision, Machines Have Entered the Real World



Source: BCG analysis.

pabilities—the hallmark of human intelligence. Today's robo-car, for example, doesn't exhibit what we would consider common sense, such as abandoning an excursion to assist a child who has fallen off her bicycle. But when properly applied, AI excels at performing many business tasks quickly, intelligently, and thoroughly.

Artificial intelligence is no longer an elective. It is critical for companies to figure out how humans and computers can play off each other's strengths as intertwined actors to create competitive advantage.

The Evolution of Competitive Advantage

In simpler times, a technology tool, such as Walmart's logistics tracking system in the 1980s, could serve as a source of advantage. AI is different. The naked algorithms themselves are unlikely to provide an edge. Many of them are in the public domain, and businesses can access open-source software platforms, such as Google's TensorFlow. OpenAI, a nonprofit organization started by Elon Musk and others, is making AI tools and research widely available. And many prominent AI researchers have insisted on retaining the right to publish their results when joining companies such as Baidu, Facebook, and Google.

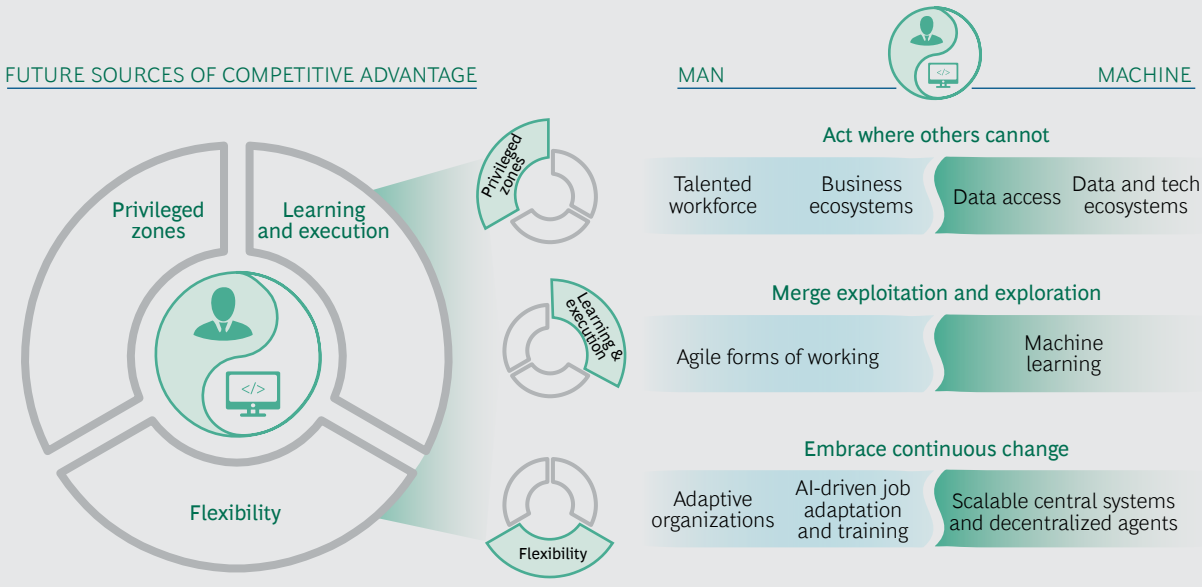
Rather than scrap traditional sources of competitive advantage, such as position and capability, AI reframes them. (See Exhibit 2.) Companies, then, need a fluid and dynamic view of their strengths. Positional advantage, for example, generally focuses on relatively static aspects that allow a company to win market share: proprietary assets, distribution networks, access to customers, and scale. These articles of faith have to be reimagined in the AI world.

Let's look at three examples of how AI shifts traditional notions of competitive advantage.

- **Data.** AI's strongest applications are data-hungry. Pioneers in the field, such as Facebook, Google, and Uber, have each secured a "privileged zone" by gaining access to current and future data, the raw material of AI, from their users and others in ways that go far beyond traditional data harvesting. Their scale gives them the ability to run more training data through their algorithms and thus improve performance. In the race to leverage fully functional self-driving cars, for example, Uber has the advantage of collecting 100 million miles of fleet data daily from its drivers. This data will eventually inform the company's mobility services. Facebook and Google take advantage of their scale and depth to hone their ad targeting.

  Not all companies can realistically aspire to be Facebook, Google, or Uber. But they

EXHIBIT 2 | Competitive Advantage That Leverages Man and Machine



Source: BCG analysis.

do not need to. By building, accessing, and leveraging shared, rented, or complementary data sets, even if that means collaborating with competitors, companies can complement their proprietary assets to create their own privileged zone. Sharing is not a dirty word. The key is to build an unassailable and advantaged collection of open and closed data sources.

- **Customer Access.** AI also changes the parameters of customer access. Well-placed physical stores and high-traffic online outlets give way to customer insights generated through AI. Major retailers, for example, can run loyalty, point-of-sale, weather, and location data through their AI engines to create personalized marketing and promotion offers. They can predict your route and appetite—before you are aware of them—and conveniently provide familiar, complementary, or entirely new purchasing options. The suggestive power of many of these offers has generated fresh revenue at negligible marginal cost.

- **Capabilities.** Capabilities traditionally have been segmented into discrete sources of advantage, such as knowledge, skills, and processes. AI-driven automation merges these areas in a continual cycle of execution, exploration, and learning. As an algorithm incorporates more data, the quality of its output improves. Similarly, on the human side, agile ways of working blur distinctions between traditional capabilities as cross-functional teams build quick prototypes and improve them on the basis of fast feedback from customers and end users.

  AI and agile are inherently iterative. In both, offerings and processes become continuous cycles. Algorithms learn from experience, allowing companies to merge the broad and fast exploration of new opportunities with the exploitation of known ones. This helps companies thrive under conditions of high uncertainty and rapid change.

In addition to reframing specific sources of competitive advantage, AI helps increase the rate and quality of decision making. For specific tasks, the number of inputs and the speed of processing for machines can be millions of times higher than they are for humans. Predictive analytics and objective data replace gut feel and experience as a central driver of many decisions. Stock trading, online advertising, and supply chain manage-

HOW MACHINES THINK AND ACT

Three milestone events made the general public aware of AI. Each one illustrates key aspects of the technology.

Deep Blue's Defeat of World Chess Champion Garry Kasparov in 1997. Chess was originally considered an exercise that captures the essential tactical and strategic elements of human intelligence, and so it became the standard by which new AI algorithms were tested. For decades, programmers made little progress in defeating human players. But in 1997, Deep Blue, a computer developed by IBM, won the match against the world champion. Still, many people were disappointed when they realized that solving chess was not the same as solving artificial general intelligence. They did not like that Deep Blue relied heavily on brute force and memory. The program did not learn and certainly did not excel at any task but chess.

The event, however, revealed two important lessons. First, machines solve problems differently than people do. Second, many "intelligent" tasks are ultimately narrow and so can be solved by specialized programs.

With AlphaGo's 2016 victory over Lee Sedol in Go, computer dominance of board games was complete. AlphaGo, developed by DeepMind Technologies, relied on *deep learning*—a neural network, or computational brain, with multiple layers—to beat a Go world champion. An intriguing fact about this match was how the machine prepared: having run out of human games to study, it spent the final months before the match playing against itself.

Watson's Victory over Top *Jeopardy* Champs in 2011. By winning this challenging game show, IBM's Watson effectively passed a Turing test of human-like intelligence. The performance showcased state-of-the-art speech recognition, natural-language processing, and search. The victory, however, was clinched by a different skill: Watson outperformed the other contestants in the "Daily Doubles," in which players can wager all or part of their current winnings to secure a decisive lead. Making the best bet requires fast sequential reasoning, knowledge of game theory, and an ability to calculate probabilities and outcomes correctly. All these are areas in which humans are notoriously weak, as the Nobel laureate Daniel Kahneman observed in his famous book *Thinking, Fast and Slow.* Machines, on the other hand, think fast and fast in making data-heavy decisions.

Google's Demonstration of a Self-Driving Car in 2012. Google is not the pioneer of self-driving cars. That distinction arguably goes to Ernst Dickmanns, a German computer vision expert who rode 1,785 kilometers in autonomous mode on a German autobahn in 1995, reaching speeds above 175 kilometers an hour.

Dickmanns, however, never had to turn left. In their 2004 book *The New Division of Labor,* Frank Levy and Richard Murnane argue that "executing a left turn against oncoming traffic involves so many factors that it is hard to imagine discovering the set of rules that can replicate a driver's behavior." Google's self-driving car, however, routinely managed this exercise without incident. The car combined robots, computer vision, and real-time data processing to produce the ultimate intelligent agent that was capable of both exploring and learning from the real world.

ment and pricing in retail have all moved sharply in this direction.

To be clear, humans will not become obsolete, even if there will be dislocations similar to (but arguably more rapid than) those during the Industrial Revolution. First, you need people to build the systems. Uber, for instance, has hired hundreds of self-driving vehicle experts, about 50 of whom are from Carnegie Mellon University's Robotics Institute. And AI experts are the most in-demand

hires on Wall Street. Second, humans can provide the common sense, social skills, and intuition that machines currently lack. Even if routine tasks are delegated to computers, people will stay in the loop for a long time to ensure quality.

In this new AI-inspired world, where the sources of advantage have been transformed, strategic issues morph into organizational, technological, and knowledge issues, and vice versa. Structural flexibility and agility—for both man and machine—become imperative to address the rate and degree of change.

Adaptive and agile ways of working are mandatory for AI-enabled processes.

Scalable hardware and adaptive software provide the foundation for AI systems to take advantage of scale and flexibility. One common approach is to build a central intelligence engine and decentralized semiautonomous agents. Tesla's self-driving cars, for example, feed data into a central unit that periodically updates the decentralized software.

Winning strategies put a premium on agility, flexible employment, and continual training and education. AI-focused companies rarely have an army of traditional employees on their payroll. Open innovation and contracting agreements proliferate. As the chief operating officer of an innovative mobile bank admitted, his biggest struggle was to transform members of his leadership team into skilled managers of both people and robots.

Getting Started

Companies looking to achieve a competitive edge through AI need to work through the implications of machines that can learn, conduct human interactions, and engage in other high-level functions—at unmatched scale and speed. They need to identify what machines do better than humans and vice versa, develop complementary roles and responsibilities for each, and redesign processes accordingly. AI often requires, for example, a new structure, of both centralized and decentralized activities, that can be challenging to implement. Finally, companies need to embrace the adaptive and agile ways of working and setting strategy that are common at startups and AI pioneers. All companies might benefit from this approach, but it is mandatory for AI-enabled processes, which undergo constant learning and adaptation for both man and machine.

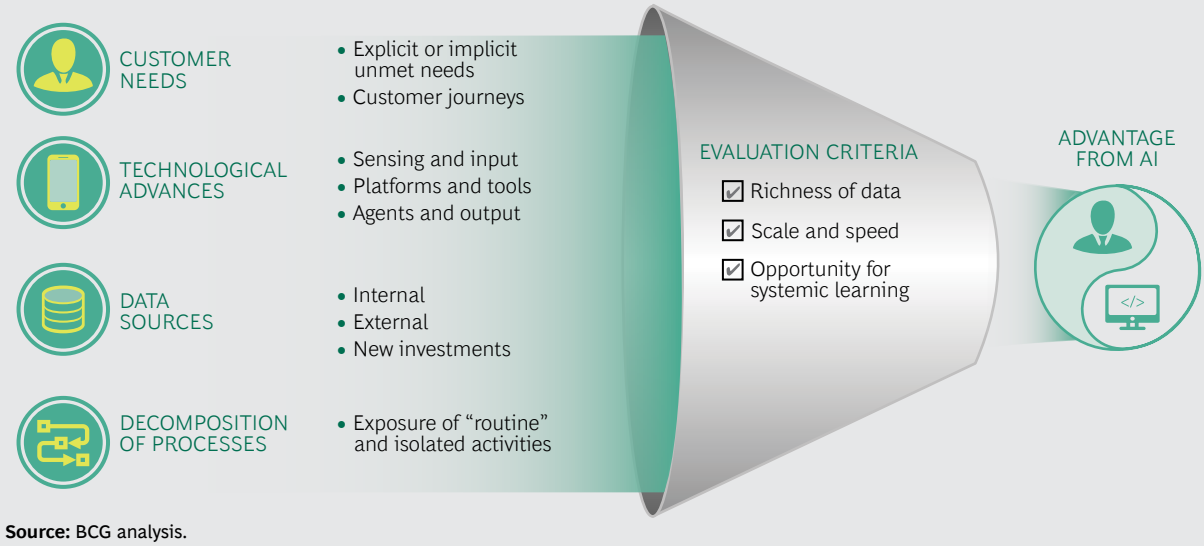
Executives need to identify where AI can create the most significant and durable advantage. At the highest level, AI is well suited to areas with huge amounts of data, such as retail, and to routine tasks, such as pricing. But that heuristic oversimplifies the playing field. Increasingly, all corporate activities are awash in data and capable of being broken down into simple tasks. (See Exhibit 3.) We advocate looking at AI through four lenses:

- Customer needs
- Technological advances
- Data sources
- Decomposition of processes

First, define the needs of your customers. AI may be a sexy field, but it always makes sense to return to the basics in building a business. Where do your current or potential customers have explicit or implicit unmet needs? Even the most disruptive recent business ideas, such as Uber and Airbnb, address people's fundamental requirements.

Second, incorporate technological advances. The most significant developments in AI generally involve assembling and processing new sources of data and making partially autonomous decisions. Numerous services and platforms can capture incoming data from databases, optical signals, text, and speech. You will probably not have to build such systems yourself. The same is true on the back end as a result of the increasing availability of output technologies such as digital agents and robots. Consider how you can use such technologies to transform your processes and offerings.

EXHIBIT 3 | Four Lenses to Shape Advantage from AI



Source: BCG analysis.

Third, create a holistic architecture that combines existing data with new or novel sources, even if they come from outside. The stack of AI services has become reasonably standardized and is increasingly accessible through intuitive tools. Even nonexperts can use large data sets.

Finally, break down processes and offerings into relatively routinized and isolated elements that can be automated, taking advantage of technological advances and data sources. Then, reassemble them to better meet your customers' needs.

For many organizations, these steps can be challenging. To apply the four lenses systematically, companies need to be familiar with the current and emerging capabilities of the technology and the required infrastructure. A center for excellence can serve as a place to incubate technical and business acumen and disseminate AI expertise throughout the organization. But ultimately, AI belongs in and belongs to the businesses and functions that must put it to use.

Only when humans and machines solve problems together—and learn from each other—can the full potential of AI be achieved.

Philipp Gerbert *is a senior partner in the Munich office of The Boston Consulting Group and a BCG Fellow analyzing the impact of artificial intelligence on business. You may contact him by e-mail at gerbert.philipp@bcg.com.*

Jan Justus *is a principal in the firm's Munich office and an active member of the Strategy practice with a focus on digital transformation. You may contact him by e-mail at justus.jan@bcg.com.*

Martin Hecker *is a senior partner in BCG's Cologne office and the leader of the Technology Advantage practice's artificial intelligence work. You may contact him by e-mail at hecker.martin@bcg.com.*

Q&A

LOOKING INTO THE FUTURE OF ARTIFICIAL INTELLIGENCE

AN INTERVIEW WITH IDSIA'S JÜRGEN SCHMIDHUBER

Jürgen Schmidhuber, the scientific director of SUPSI's Dalle Molle Institute for Artificial Intelligence (IDSIA), in Switzerland, has been a leading pioneer of artificial intelligence (AI) for three decades. His work with colleagues on recurrent neural networks, including long short-term memory (LSTM), and on other mathematical models and algorithms for solving AI problems has revolutionized several fields, including machine learning, handwriting and speech recognition, machine translation, and image captioning. These methods are now being applied in a wide variety of smart devices, including billions of smartphones, as well as in robotics. Teams led by Schmidhuber have been publishing research on AI applications for fields as diverse as art, medicine, and music—while he continues the quest he began in the 1980s to develop general problem solvers. BCG senior partner and managing director Philipp Gerbert recently sat down with Schmidhuber to discuss his views on the present and future of AI.

Jürgen, it's a privilege to have you here as one of the pioneers of artificial intelligence and, more specifically, deep learning—it's the hottest field right now. Before you go into all of that, we would like to understand the person Jürgen Schmidhuber better. Perhaps you can tell us a few things that you're particularly proud of in your career.

One of the things I'm proud of: I think I understand what it means to be curious and how to implement curiosity, which I think is essential to build agents that learn from experience through their own self-generated experiments. Agents that are motivated to invent, in a directed way, action sequences or experiments that lead to data that tell them something about how the world works that they didn't know yet. If you Google "artificial curiosity," you will end up on our pages and learn all about that.

Another question I have, which often tells what people stand for, is this: What is something you believe in, but you think that 95% of humanity would not?

Since the 1970s and 1980s, I have believed that intelligence is a simple thing and that, in the end, all of the essence of intelligence can be condensed into a short code—ten lines of pseudocode or something—which includes everything that you need to build a continually self-improving system. My first publication

JÜRGEN SCHMIDHUBER

Jürgen Schmidhuber is the scientific director of SUPSI's Dalle Molle Institute for Artificial Intelligence (IDSIA), in Switzerland. He is also the president of NNAISENSE. In 2016, he was awarded the IEEE Neural Networks Pioneer Award and the NVIDIA Pioneers of AI Research Award. He holds degrees from the Technical University of Munich, where he also previously served as head of the cognitive robotics lab and professor of cognitive robotics.

on that with concrete algorithms dates back to 1987, to my diploma thesis. In the past 30 years, I have kept working on this grand problem of AI, and I think we are rather close to the final solution.

You say intelligence might be a simpler concept than most people think. But many struggle with what artificial intelligence really means. Could you explain it to us?

All of natural intelligence and artificial intelligence is about problem solving. In AI, we are trying to build general problem solvers that can solve not only one little problem here and one little problem there but many, many different problems that are practically irrelevant in this initially unknown environment we are living in. We want to build machines and robots and agents that learn to deal with basically arbitrary, initially unknown environments and then learn to solve pretty much arbitrary problems within these environments.

There's a lot of hype right now. What do you feel are things that are really exaggerated, and where might there be things that are still underappreciated about AI in the current environment?

I don't think that there are too many exaggerations right now. At the moment, we are still experiencing this trend that basically says that every five years, computing gets ten times cheaper. That trend has held since 1941, when Konrad Zuse built the first working program-controlled computer. At the moment, we still have rather small neural networks compared with the human cortex.

You have 100,000 times more connections than one of these little artificial networks. However, this is just a period of 25 years, which means that by 2041, we should be able to get, for the same price, large LSTM networks that can compute or that have as many connections as a human cortex, and these will be much faster than the wet connections I have in here because these will be electronic connections. So even if there are no additional algorithmic breakthroughs, we will still see lots of superhuman performance results by just scaling the existing things up through the faster hardware.

Right now, speech and text recognition is being solved, so a lot of human knowledge becomes accessible to machines. At the same time, vision allows computers to navigate the real world. That obviously leads to lots of fears about the ability of humans to adapt to these changes so fast, since timescales have decreased. Any view that you might have on this subject?

Predictions of job losses through robotics are old. Many decades ago, people predicted that robots were going to take over all kinds of jobs. But then what happened is that those countries where there are lots of robots per million capita, they all have low unemployment rates. Countries such as Japan, Germany, Korea, Switzerland have many robots per capita by international standards but rather small unemployment rates. It's easy to predict which jobs are going to disappear, but it's hard to predict which new jobs are being created.

If you look a bit further in the future and see that there might be real superintelligence, is it potentially dangerous? And can we or should we slow down our efforts to develop this?

In the long run, AIs are going to be much smarter than humans. Should we be afraid of them? I don't think so, because most beings are mostly interested in those who are similar to themselves. Look at yourself, you are mostly interested in other humans like yourself because with those you can either collaborate to achieve goals or you can compete. You share goals, and that's the reason why you are interested in these potential competitors or collaborators. That's the reason why most politicians are interested in other politicians, and most reporters are interested in other reporters, and most frogs are interested in other frogs. And those superintelligent AIs of the future will be mostly interested in other superintelligent AIs of the future. And not so much in frogs and humans and ants, just like you are not so interested in all of these ants out there. Just because you are smarter than the ants, you are not going to kill them. No. The weight of all of the ants on this planet is still comparable to the weight of all humans, and there are still many, many more ants out there than humans.

Jürgen, thank you very much for this very interesting interview. The good news is that we definitely continue to live in interesting times, and I would enjoy continuing the discussion. Thank you very much.

Philipp Gerbert *is a senior partner and managing director in the Munich office of The Boston Consulting Group and a BCG Fellow analyzing the impact of artificial intelligence on business. You may contact him by e-mail at gerbert.philipp@bcg.com.*

FIVE LESSONS ON DIGITAL TRANSFORMATION FROM B2C LEADERS

by Claude Czechowski, Guillaume Combastet, and Antoine Gourevitch

COMPANIES' LIFESPANS ARE SHORTER than ever before. Digital disruption has become so intense that pure players in digital are no longer disrupting just incumbents, they are disrupting other pure players as well: HomeAway has emerged as a strong rival to Airbnb. Apple Music is nipping at the heels of Spotify's streaming music service. The tech giants—Google, Apple, Facebook, and Amazon—are in the driver's seat, setting new standards for digital.

Digital disruption has grown so intense that pure players in digital are disrupting other pure players.

To understand how leading companies are responding to the dynamism and unpredictability of today's marketplace, The Boston Consulting Group partnered with IBM and Electronic Business Group, a leading French think tank, to interview the leaders of 70 B2C companies (60 incumbents and 10 leading pure digital players) on the topic of digital transformation.

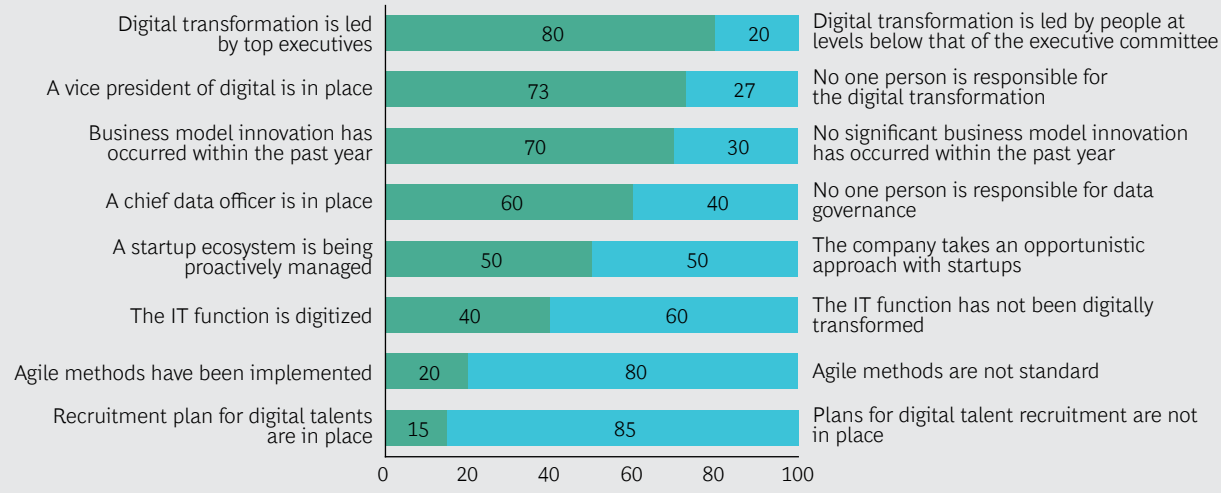
The results are striking. With new attackers appearing all the time, digital transformation is seen by many as the only path to survival. But while many companies are restructuring their governance to become digital ready, there is still much to be done in terms of implementing agile at scale, capitalizing on open innovation, and hiring new digital talent. (See Exhibit 1.)

Where Companies Are Today

Every industry is impacted by digital, but companies' approaches to it vary according to how much pressure they experience from new entrants and the extent to which digital is transforming their particular sector. (See Exhibit 2.) Some sectors, such as hospitality, retail, and travel, are already contending with intense competition from digital start-ups, many of which are flush with cash from venture capitalists. Others, such as banking and insurance, are playing defense because they are at least somewhat protected by legal barriers that make it hard for new entrants to gain traction, though banks are heavily under attack from financial technology companies, particularly in the area of payments. The luxury and consumer packaged goods (CPG) sectors are facing stiff competition from new entrants; without legal protections, these companies are being forced to adapt rapidly.

In response, most incumbents now regularly scan the horizon for new technologies and patents to acquire attackers before they become too dangerous. Unilever's $1 billion ac-

EXHIBIT 1 | The State of Digital Transformation for B2C Companies in 2016



Sources: Interviews with 70 digital leaders and C-suite executives of B2C companies; BCG analysis.

quisition of Dollar Shave Club offers a striking example of this strategy in action.

In all sectors, the pressure to digitally transform the business is only getting more intense owing to five trends:

- **Evolving Customer Behaviors.** Digital newcomers are transforming customers' expectations. Users want a simple, fast, user-friendly digital experience in all of their online transactions, but most say that they are dissatisfied with their online experiences. Companies need to reinvent their customer engagement model to allow seamless switching between channels, mobile-friendly services, and first-time fixes (with no handoffs).

- **Technological Leaps.** Increased connectivity and mobility, cloud-based services, artificial intelligence, and the Internet of Things are helping companies improve efficiency in almost every aspect of the business, including digital marketing, manufacturing, R&D, and supply chain.

- **Data Explosion.** The increasing volume and diversity of data generated through digital channels are providing companies with valuable market insights that inform real-time, data-driven decision making and improve customer targeting.

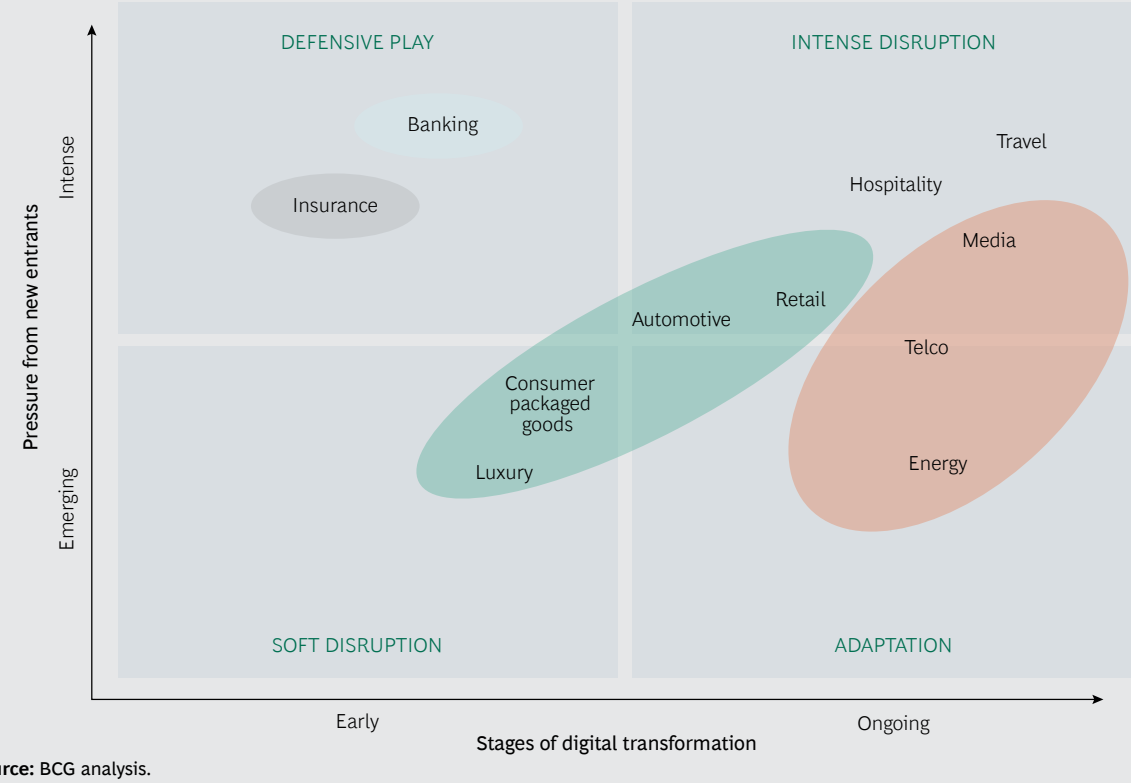
- **Legal Factors.** In some sectors, laws and regulations constrain incumbents by lowering competitive barriers for new entrants. Conversely, laws and regulations that deter new entrants can protect incumbents. New laws can also provide a strong incentive for innovation. In the automotive industry, for example, heightened emissions standards have supported greater investment in fuel-efficient hybrid or electric vehicles.

- **Pricing.** Many startups are focused above all on moving quickly to gain market share, not turn a profit, which can put significant pressure on incumbents' margins. In this environment, it's more important than ever for companies to reduce costs, improve efficiency, and explore new ways of generating revenue.

With so many factors in play, companies need to set a bold course toward digital transformation. Some have already begun to do so: more than 70% of the executives we surveyed said that they have named a chief digital officer who stays alert to disruptive threats and opportunities and drives a digital-first agenda. More than 60% have launched a startup incubator, and 45% have invested in new ventures.

Nevertheless, more remains to be done.

EXHIBIT 2 | Pressure from New Entrants Forces Incumbents to Accelerate Their Digital Journey



Source: BCG analysis.

Where Companies Need to Be

To capture the full value of digital, companies must advance five fundamental strategies.

Harness the power of data. With an endless stream of data flowing from smartphone apps, website browsing, social media messages, and customer transactions of all kinds, companies have enormous opportunities to harness the power of big data. But this data must be stored and managed such that it yields accurate predictive modeling and meaningful customer insights. Enterprise data warehouses, commonly called data lakes, can be used to store and structure data from multiple sources into a single repository, and they can model the data so that it supports decision making, research, and innovation.

Companies also need to hire the right talent, such as data scientists, to gain an edge in analytics and create tangible value for the business. For example, AXA Equitable Financial Services, the multinational insurance firm, hired approximately 60 data scientists to fuel data-driven innovation and respond to requests from affiliates. They are supported by data specialists in charge of embedding culture throughout the company to ensure that data is being mined across business units.

Redefine the customer journey. The customer journey is more complex than ever. Today's consumers have become accustomed to 24-7 availability and seamless interactions across platforms and devices, and they have very limited tolerance for service delays and handoffs. To meet these demands, companies—whether B2C, B2B, or B2B2C—need to put the end user at the center of their enterprises, which means mapping the customer journey, identifying customer pain points, developing prototypes, and testing solutions. This kind of "design thinking" approach allows companies to create a superior user experience. The bank Crédit Agricole, for example, has created a multichannel model that meets clients where they are—moving fluidly between online and offline channels. First contacts are almost 100% mobile, and bank advisors equipped with tablets routinely travel to client sites for in-person visits. Companies that get this effort right will find themselves with a legion of loyal consumers.

Build digital capabilities throughout the enterprise. Digitization is not an add-on. Rather, it is a fundamental transformation of the core business, which includes functions as diverse as logistics, supply chain, operations, and the back office. Companies have the opportunity to create digital factories that simulate an entire production process. Such digital simulation can be used, for example, to optimize factory layout, identify and correct flaws in the production process, and model product quality. Furthermore, cloud-based solutions, application programming interfaces, and agile operations can be used to improve flexibility and time to market. Companies also need to manage IT by implementing new digital platforms and integrating them with legacy systems. Total, the international oil and gas company, has achieved this by establishing a digital IT team with a "fast and flex" structure to manage continuous IT delivery and rapid prototyping, while the legacy IT team integrates apps into core enterprise resource planning.

Transform governance and explore collaborative ways of working. To move at the speed that digital requires, companies must adopt a new way of working. Cross-functional teams must collaborate to brainstorm ideas, conduct prototyping, run A/B testing, and incorporate user feedback. This, in turn, will require a new form of governance, in which teams are given more autonomy. While corporate management defines global goals and sets strategic objectives (for instance, capturing a greater percentage of business online by 2020), local teams are given the freedom to operate in a way that ensures they maintain the optimum speed and contribute to corporate objectives. In some cases, companies may want to jumpstart the digital transformation by developing partnerships with digital players. For example, Danone, the global food company, created a digital board—including the chief data officer, the chief information officer, and the chief human resources officer—to work in concert with the executive committee. The board aligns on overall objectives but allows local divisions to develop their own content.

Reinforce innovation capabilities. It's important for companies to carry out their digital transformations across three dimensions: transforming the core to be more digitally sophisticated, restructuring the business to become more agile and flexible, and exploring new avenues for breakthrough innovation. To make headway in all three areas, companies should explore new opportunities that arise with regard to open innovation, incubators, innovation centers, and corporate ventures. Many companies have successfully named (or hired) a chief disruption officer to drive change and safeguard the business against emerging digital attackers. Diageo, a global premium drinks business, has deployed a wide variety of innovation capabilities, including agile processes, prototypes, the ability to scale up new products in less than 18 months, and corporate ventures that monitor the startup ecosystem and accelerate acquisitions.

DIGITIZATION, automation, the Internet of Things, and other technological advances are rapidly changing the global economy, and companies that fail to evolve are at risk. Digital attackers are going after the most profitable parts of incumbents' businesses, disconnecting them from their customers, stripping away profit centers, and leaving incumbents to manage activities that are more costly and less valuable (as we've seen with payments processing in banking). For companies that develop digital capabilities too late, the shakeout can be merciless. With these five strategies in their arsenal, CEOs have an opportunity to drive successful digital transformations and reshape their companies' digital destinies.

Claude Czechowski *is a senior advisor in The Boston Consulting Group's Technology Advantage practice and digital transformation topic. He has coached CEOs in France, Germany, and the UK and guided digital strategy for several large financial services corporations. You may contact him by e-mail at czechowski.claude@advisor.bcg.com.*

Guillaume Combastet *is a principal in the firm's Paris office and a core member of BCG's Technology Advantage practice. You may contact him by e-mail at combastet.guillaume@bcg.com.*

Antoine Gourevitch *is a senior partner and managing director in BCG's Paris office. You may contact him by e-mail at gourevitch.antoine@bcg.com.*

Q&A

DIGITAL TRANSFORMATION—FROM BLACK BOX TO CRYSTAL CLEAR

AN INTERVIEW WITH ROLAND HARSTE, SENIOR VICE PRESIDENT FOR GLOBAL MARKETING, SWAROVSKI

Roland Harste is the senior vice president for global marketing at Swarovski, a producer of cut crystals and crystal products since 1895. In addition to his core marketing role, he is responsible for the company's digital transformation across three departments: online marketing (website, apps, social media), B2B e-commerce, and online retail (where customers can purchase products with Swarovski crystals).

The Boston Consulting Group partnered with IBM and the Electronic Business Group, a leading French think tank, to interview digital leaders and C-suite executives on the topic of digital transformation. Harste recently sat down with Claude Czechowski, a senior advisor to BCG's Technology Advantage practice, to discuss the challenges inherent in leading a digital transformation in a global company with roots going back more than 100 years. Edited excerpts from their conversation follow.

What is the main focus of your digital transformation at Swarovski?

We sell crystals to 5,000 different B2B customers, like Prada, Armani, and Gucci, but also to many, many others in the fashion and jewelry industries. Our customers produce finished products with Swarovski crystals—shoes with crystals, for example—and then they sell them through retail channels. Not only do we sell the crystals, we also help our customers sell their products.

Our digital transformation is mainly designed to make our B2B customers successful in retail. We help them market and sell their products to their customers. As in other industries, online is becoming the dominant channel; therefore, it is very important for us to have scalable digital platforms through which we can help them sell products with Swarovski crystals.

We have 15,000 different SKUs for loose crystals and another 200,000 crystal products. In addition, because there are so many different application techniques, our crystals can be used in more than 1 million combinations. When customers want to use our crystals, they need to navigate effectively through our vast assortment. So, we created the Crystal Collection App, a digital catalog that lets consumers navigate through our whole assortment. This is great for our customers, and we also get live

ROLAND HARSTE

Roland Harste, the senior vice president for global marketing at Swarovski, is the youngest designated member of Swarovski's core management team, which includes the top six executives overseeing approximately 4,500 employees within the professional business unit. He studied economics, industrial engineering, and management at the European Business School Oestrich-Winkel, INSEAD Fontainebleau, and Hamburg University of Technology.

streams of transactional data that show what they are looking for and allow us to develop customer-specific recommendations that our key account managers can use in their B2B interactions.

We are also developing an e-commerce solution to sell all our loose crystals to B2B customers. The thing that's tricky for us is that we sell directly to B2B customers, but we also sell indirectly through wholesalers. With our e-commerce solutions, we basically become competitors of our own indirect customers. This has been a big challenge from an organizational perspective. For the sales team, it felt like a huge channel risk. Are we crazy to compete against our own customers? How do I manage my own account and the revenue coming from the e-commerce solution, which is managed through headquarters? How does that feed into my net sales in the country? These discussions have kept us busy for a year and a half.

How has your B2C business evolved from a digital perspective?

The goal on the B2C side is to make our ingredient brand strong. Let's take Jimmy Choo, for example. The Jimmy Choo company wants to crystallize a shoe and sell it in retail. It's a Jimmy Choo shoe with ingredients—crystals—from Swarovski. The company can use a Swarovski tag or a seal on its product and use our brand in its communications.

But when it comes to digital communication, it's important for us to make people aware of the ingredient brand. For example, Swarovski sponsors the Victoria's Secret fashion show. If we do something with Victoria's Secret, we create more than 100 million impressions and we get huge engagement on social media. In the end, if a consumer wants to purchase a product with Swarovski crystals, she may not find it. Why? Because online retailers may not include the right keywords when they categorize products. If they don't say that the ingredients are from Swarovski, there's no way for someone seeking a product with Swarovski crystals to find it.

The biggest challenge in Swarovski's digital transformation? The mindset shift.

So, our digital solution was to develop a crystal hub [www.crystals-from-swarovski.com]. In our crystal hub, consumers can say, for example, "I want to see all shoes that include Swarovski crystals." The consumer can see different brands of shoes, find the product, and then say, "I want to purchase this product." We then lead the consumer to an online retailer, which handles fulfillment. This is very interesting because it will help our B2B customers sell products with Swarovski crystals to their customers.

How much value do you expect to create through e-commerce?

We have very big customers in B2B, and they will still be served through the normal offline channels. Our e-commerce is more for the smaller customers. So I expect we'll have just 3% to 5% of our total revenue coming from e-commerce in three years or so. With B2C, the revenue stream is a little different because we don't own the finished product for Swarovski crystals. If we help a customer sell 1,000 products, each of which costs €500, we don't get €500,000; we get only the crystal share. For us, the bigger net sales advantage in B2C is in providing a service to our B2B customers. We provide a distribution platform and create loyalty. That's more important to us.

In 2017, we will develop a marketplace where we own the customer relationship. We are one of the biggest jewelry manufacturers in the world, and we have 1,300 of our own Swarovski stores and 11,000 points of sale. If we can use that distribution and our loyalty program to drive traffic to our crystal hub, this would be a tremendous value.

Have you had success partnering with startups?

We have an open innovation team with a huge network of startups. If we need a specific technology—like a tool to manage product feeds from the online retailers for our crystal hub, for example—these startups have the technology and experience. There are so many new technologies that it's not so difficult to get information about what's out there and what we can use. The more difficult thing is to have a clear strategy and understand what's relevant for the business, how to monetize it, and how to integrate it into existing processes.

What are some of the challenges you've faced over the course of Swarovski's digital transformation?

The biggest thing is the mindset shift. We are a very old business. Swarovski started more than 120 years ago and has been very much

an offline relationship business. We needed to get into the mindset that digital is important. Everybody understands advertising and building the brand through social media, but when it comes to commercialization and e-commerce, for example, that's a huge mindset change for the organization. It's very important that the people driving the digital-transformation agenda use every opportunity to talk to the business. We have had lunch lectures where people can participate and better understand the objectives, and they become more open to digital in the end, which is very important.

Who is driving the digital transformation? The CEO? Or a business unit?

Much of it comes from the marketing side. For me, it's logical that we use e-commerce as a lead generation channel and to better understand our small customers, which were kind of a black box for us in the past.

But the question of who drives everything is complicated. Where does e-commerce sit and who develops it? For us, e-commerce is developed in the marketing organization, but it could have been in sales or in a separate digital business. Furthermore, we should not underestimate the importance of adjacent functions, such as supply chain, IT, and finance. How do the P&Ls work together in the offline and online business? How do we incentivize our sales force to send small customers to the e-commerce shop? And when customers are big enough, they need to be sent back to the offline sales organization. It's very important to get alignment on these points.

Which teams are driving the company's digital transformation?

From an organizational point of view, we have many different business units involved in the digital transformation: marketing, IT, the consumer business, etcetera. Everybody wants to drive the digital-transformation agenda. IT developed the digital-transformation agenda from a technical point of view. Other business units developed an agenda from their points of view. We are now in the alignment process, to bring all these together. In the offline world, the business units could operate separately. But it's not possible anymore to tell the consumer, "Go to the sales organization," because we have so many touchpoints now. In a digital environment, we have to provide one view to the consumer. I'd say we're at about 80% in terms of alignment. There are still some really big nuts to crack, but these are more on the organization side, like having one customer loyalty program and getting the best people on board.

The most difficult thing for us was to get the right profiles on board. If you want to get into e-commerce, it's not easy to find the right people because there's huge competition. It's so important to get really great people on board who have a network. That gives the organization credibility—people start to see that something big is happening— and then you get more people.

Have you integrated the data and analytics as well?

I would say we are at about 30% on data and analytics. We have tons of data. Through the Crystal Collection App, for example, we have so much transactional data from many different channels. We still need to create one view, but we have made a big step forward now that we have one customer relationship management system.

Another difficult thing is how to make use of the data. How do you bring it back to the consumer to create a cross-sell, an up-sell, or better lifetime value?

I'll give you an example.

Our Crystal Collection App allows B2B customers to search through our product assortment to view a specific crystal by color, size, and cut. Our key account managers can now see transactional data based on past purchases and customers with similar purchase patterns, and they can make recommendations to the customer. That would be a great use case. But to make that happen, we have to get the key account managers to use the iPad with customers, understand how it can be used in the selling discussion, and so on. I think the most difficult part is to persuade key account managers to use it. You can analyze data until you are dead, but you need to create use cases, and behind each use case there needs to be an understanding of how to create more value for the business. Everything else should follow from this.

Claude Czechowski *is a senior advisor in The Boston Consulting Group's Technology Advantage practice and digital transformation topic. He has coached CEOs in France, Germany, and the UK and guided digital strategy for several large financial services corporations. You may contact him by e-mail at czechowski.claude@advisor.bcg.com.*

WINNING IN IOT

IT'S ALL ABOUT THE BUSINESS PROCESSES

By Nicolas Hunke, Zia Yusuf, Michael Rüßmann, Florian Schmieg, Akash Bhatia, and Nipun Kalra

The B2B market for the Internet of Things (IoT) is taking off. And huge numbers of vendors—including software, hardware, and internet companies; startups; service providers; and telcos—are jockeying for position and market share. With so much action in the IoT space, one question should be at the top of every IoT provider's list of concerns: Where are the growth opportunities?

To understand how IoT is being deployed by businesses today—and where the major growth opportunities will be in the future—we analyzed trends currently shaping the IoT landscape. Our analysis uncovered three major findings. One, there is no such thing as "the" Internet of Things: today's market is heavily driven by specific use case scenarios. Two, while in the aggregate, companies will spend an incremental €250 billion on IoT in 2020 (over and above their normal technology spending), three industries will account for approximately 50% of that spending. And three, although all layers of the IoT technology stack are poised to grow through 2020, the layers are not equally attractive.

Growth Opportunities in IoT

From 2015 through 2020, all layers of the technology stack are expected to have achieved a compound annual growth rate of at least 20%, but certain layers have much higher growth potential than others. (See Exhibit 1.)

How are businesses deploying IoT? And where are the major growth opportunities?

IoT's real value, from the customer's perspective, is in the top two layers of the technology stack; that is, services and IoT analytics and applications. We expect that by 2020 these two layers will have captured 60% of the growth from IoT. The rest of the technology stack—identity and security, IoT backbone (cloud and platform), communications, and connected things—are enabling components with lower growth potential.

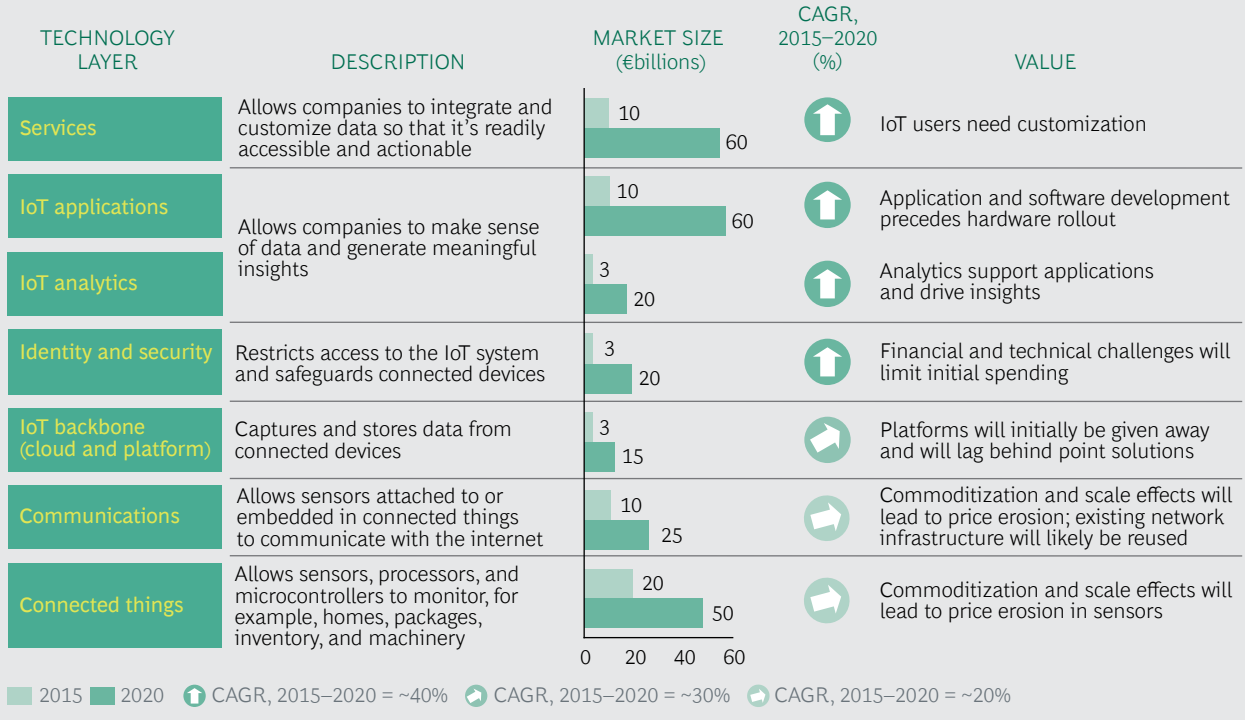
Use Cases Driving IoT Adoption

Companies will likely spend some €250 billion on IoT, but they need to know which IoT applications have the potential to deliver the most value. Determining this requires recognizing that business leaders are using IoT to solve discrete business challenges. They're asking, How can IoT help our company increase customer satisfaction, improve quality, support new business models (such as data-driven services), and reduce costs?

A few use cases are driving IoT adoption and growth and will continue to do so through 2020 at least. To gain meaningful market share over the near term, companies need to focus their IoT product offerings on the right use cases.

With this in mind, we identified a wide range of use cases for IoT. From this long list, we pinpointed

EXHIBIT 1 | Services and IoT Applications and Analytics Will Capture Some 60% of IoT Spending



Sources: IDC; Gartner; ABI Research; BCG Internet of Things buyer survey; expert interviews; BCG analysis.

ten IoT use cases that are poised to mature rapidly and experience widespread adoption (in a B2B context) through 2020. (See Exhibit 2.) Insight into where customers plan to invest in IoT, when they will invest, and how much they plan to spend helps clarify which use cases will drive IoT growth through 2020. Ten IoT use cases show the most promise.

Predictive Maintenance. Inevitably, businesses lose valuable time and money when equipment malfunctions or breaks down. And many companies also lose money each year by adhering to fixed maintenance schedules by which equipment vendors make routine calls—even when no maintenance is required. IoT technologies can predict or detect when a machine requires maintenance, reducing or eliminating unplanned downtime, extending maintenance cycles, and reducing costs. A host of industries—including utilities, discrete manufacturing, transportation and logistics, energy, and health care—can benefit from predictive maintenance. Of course, solutions need to be tailored to suit specific industry needs and applications.

Self-Optimizing Production. Connected factories and plants can use IoT to monitor and optimize production processes in real time, making automated adjustments to improve quality, enhance efficiency, and reduce waste. This use case is ideal for discrete manufacturing and process industries.

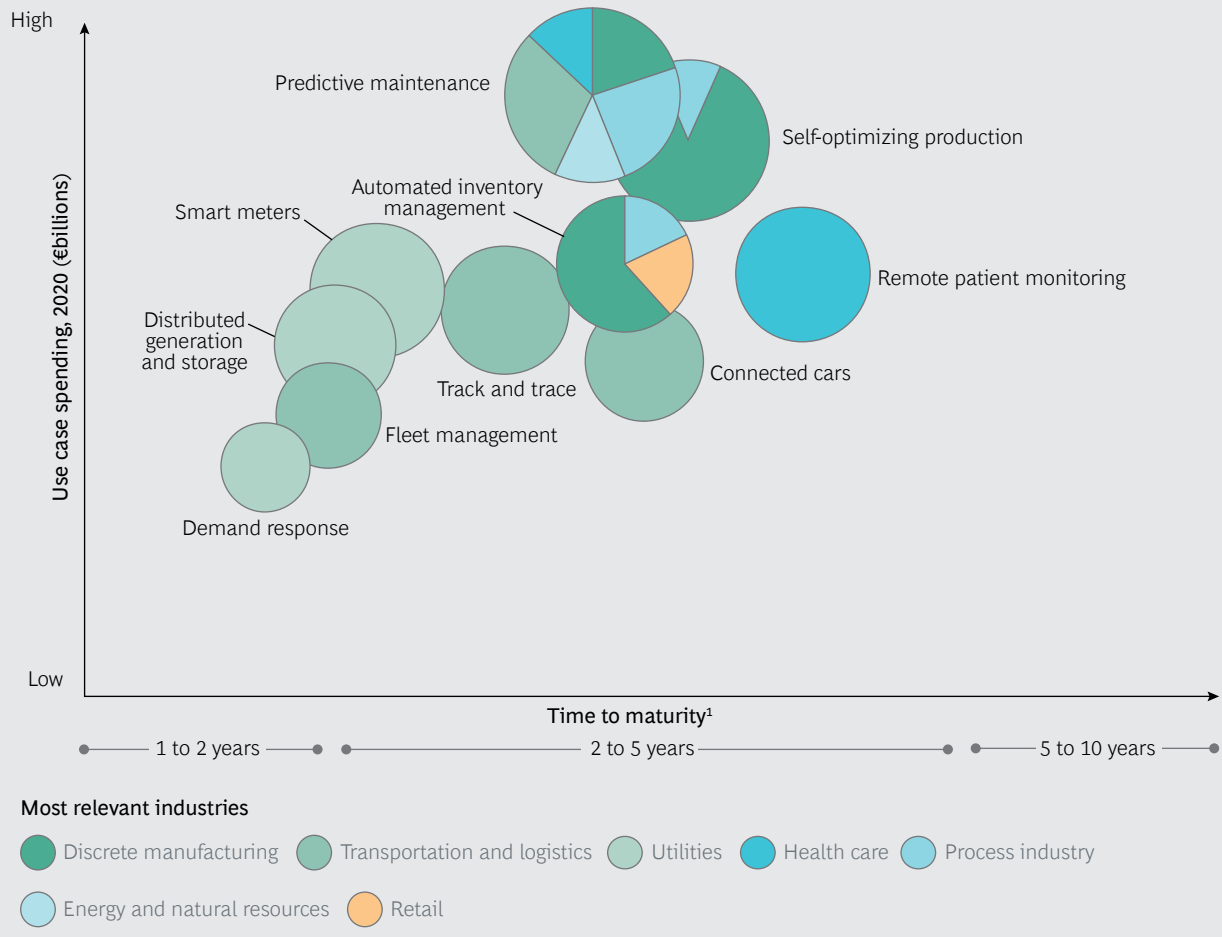
Automated Inventory Management. IoT can provide much greater insight into the status of inventory and the supply chain, allowing companies to track inventory location and condition (including, for example, temperature, humidity, and damage). The ability to monitor products across the supply chain allows companies to increase processing and response time, reduce stockouts and inventory pileups, and improve just-in-time production processes.

Remote Patient Monitoring. Physicians can track patient health remotely, in real time, to improve health outcomes and reduce health care costs. By tracking patient data and monitoring compliance, health care providers can help patients stay healthier and recover more quickly.

Smart Meters. Sensors can be used to monitor utilities—including electricity, gas, and water consumption—in real time. Smart meters can help consumers monitor their usage, reduce the number of technicians needed to read meters, provide real-time billing data, and enable more dynamic pricing.

Track and Trace. IoT sensors are ideally suited for increasing systems' efficiency. They can, for

EXHIBIT 2 | Ten Use Cases Will Drive IoT Growth Through 2020



Sources: BCG Internet of Things buyer survey; IDC; expert interviews; BCG analysis.
Note: The bubble sizes indicate relative amounts of spending.
[1]Productive and scaled use within real-life settings (that is, no pilots). To capture opportunities, vendors must quickly ramp up activities. The timing of commercial viability for these use cases was derived from responses to a survey question: "When do you expect to productively use [name of use case]?"

example, enhance transparency in order fulfillment and provide information that can help reduce workstation transition times. The sensors can be used in the assembly area to identify the status of products and to locate tools, components, and materials.

Distributed Generation and Storage. IoT can be used to automate and optimize supply and demand across multiple energy sources. By remotely monitoring and controlling distributed energy generation and storage, companies can balance energy usage across the grid and reduce energy costs.

Connected Cars. Through new types of sensors, wireless connectivity, and onboard processing units, vehicles are increasingly connected, and many consumers already expect this type of functionality. Connected cars offer enhanced navigation, better safety features, and various creature comforts, including advanced music and entertainment options. Some features of connected cars are expected to mature slowly over the next five to ten years.

Fleet Management. In addition to tracking inventory and parcels, IoT is being used to track vehicles in real time. With better information related to fleet location, usage, and condition, companies can be more efficient, reduce maintenance and repair costs, and allow for dynamic rerouting to avoid congestion and delays. This use case is expected to mature quickly—within the next one or two years.

Demand Response. IoT is starting to change the way end users interact with utilities. Through demand-response programs, customers can allow the remote control of their use of certain appliances—air-conditioning systems, washing machines, and

other energy-intensive appliances—during peak-demand periods. These processes can be automated to reduce supply and demand volatility and lower customers' energy bills.

ing, transportation and logistics, and utilities. (See Exhibit 3.)

Some use cases, such as predictive maintenance, represent a great opportunity for all industries. Still, each offering must be tailored to meet any given industry's unique needs. The expected time to maturity is significantly different for each use case, depending on its share of customers and how quickly it scales.

ers' machines run more efficiently, in 2015. Siemens, with its MindSphere platform, is pursuing a similar path. Other companies are focusing on a specific layer of the stack and making a horizontal play, as Microsoft has done with its Azure IoT Suite. The SAP HANA Cloud Platform, IBM Watson IoT Platform, and Cisco IoT System all allow companies to build and deploy their own IoT applications—and they are providing specific applications as well. Device makers, such as Intel and Bosch, are offering hardware and complementary operating systems to provide customers with a more comprehensive IoT ecosystem.

Although a wide variety of players have entered the IoT space, our survey shows that 40% of today's IoT customers prefer to use traditional and well-established software companies for their IoT solutions. In selecting an IoT software vendor, customers' top three criteria are product functionality, the vendor's reliability, and assurance that the solutions can be integrated.

This last point about integration is very important. Today's IoT cus-

> There's plenty of room for all kinds of companies to grow in IoT.

An Industry-Specific View

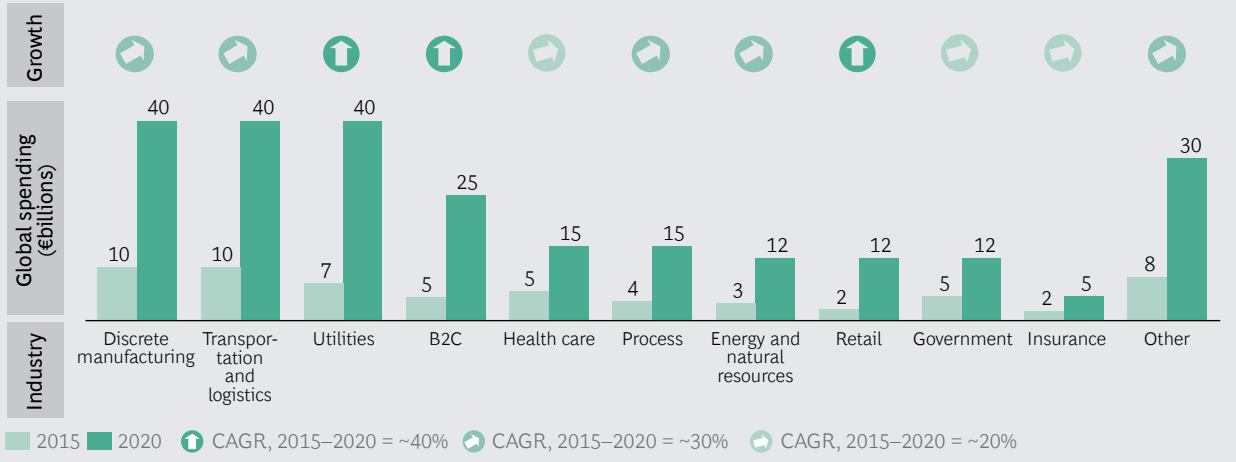
Although advanced-technology companies already have integrated digital capabilities, the same cannot be said for companies in other, more conventional businesses, such as industrial goods or logistics. IoT is certainly an important source of growth for technology companies; for less technology-centric companies, it can be utterly transformative.

By cross-referencing use cases with industries, we can see, from an industry perspective, where the most value will be created in the coming years. Three industries will likely account for approximately 50% of IoT spending: discrete manufactur-

Players and Plays

There's plenty of room for all kinds of companies to grow in IoT—and there are numerous possible ways to engage in the IoT market. Major industrial companies are increasingly transitioning from being IoT customers to being IoT providers. General Electric, for example, released Predix, an end-to-end IoT industrial operating system designed to help GE custom-

EXHIBIT 3 | IoT Spending Is Expected to Approach €250 Billion in 2020



Sources: BCG Internet of Things buyer survey; IDC; expert interviews; BCG analysis.
Note: Because of rounding, the numbers do not add up to €250 billion.

tomers are looking for end-to-end solutions. World-class applications and services deliver value only when the underpinnings (the connected things, communications, backbone, and security layers) work seamlessly with the top layers. IoT providers don't necessarily have to master all the components within the technology stack, but it is essential to craft a go-to-market plan that takes into account the customer's desire for an end-to-end solution.

Winning in IoT: Key Questions

To compete successfully, IoT vendors need to develop a strategy for where they will play and how they will win. Executives who are strategizing about where to play should respond to the following sets of questions:

- **Addressing Use Cases.** What are the company's strengths and how can these be leveraged to address use cases? Do we want to address one or more use cases within a specific industry (for example, targeted solutions for medical-device manufacturing) or build a single adaptable solution that can be used by a number of industries (automated inventory management)?
- **Targeting Customers.** What types of customers do we want to attract? Is the company better positioned to directly serve clients that operate assets (such as transportation companies that need predictive-maintenance capabilities) or should we pursue clients that manufacture IoT-ready assets for these businesses (such as large industrial manufacturers that supply products to oil and gas companies)?
- **Developing End-to-End Solutions.** What will the company offer customers? Can the company develop an end-to-end solution that covers all layers of the stack under our brand, or will we specialize in a particular layer of the stack (as a means to enable other IoT solution providers)?

IoT vendors need to develop a strategy for where they will play and how they will win.

Once an IoT vendor decides where to play, management must determine how to win in that space. As companies explore this angle, they must address the following:

- **Leveraging Partnerships.** How can the company leverage existing assets and capabilities to optimize its position within the technology stack? Is a software company, for example, well positioned to build up talent and capabilities in hardware? Or is it preferable to form strategic partnerships with other players, such as hardware companies, service providers, and systems integrators?
- **Understanding How Sensor Data Will Be Used.** In IoT, sensors can provide a flood of data, and it's critical to ensure that the data is linked to clear business objectives (such as increasing revenues and reducing costs). What business metrics will we measure once IoT sensors are in place?
- **Building Capabilities.** What new capabilities does the company need? Should we build up internal capabilities, pursue M&A, or establish partnerships?
- **Crafting a Go-to-Market Strategy.** What is our go-to-market strategy? If the company has focused mainly on B2C, for example, how should the strategy change to reach B2B customers? If the company has historically sold software to IT departments, how will we reach out to business stakeholders? IoT conversations have to be centered on use cases and business value.
- **Evolving the Business Model.** Given the granularity of available sensor data, new business models are emerging. Instead of selling equipment for an upfront fee, for example, companies get compensated for the actual use and uptime of that equipment. How can we capture more value through these new business models and create a compelling business case for our customers?

The right path forward will vary depending on each company's starting point:

- **Enterprise software companies** need to leverage their brands' strong reputation and build an end-to-end solution through M&A or partners. As far as most customers are concerned, platforms don't drive major value in IoT solutions: 80% of the IoT customers we surveyed were not at all aware that they were using a platform. Nonetheless,

platforms represent an important horizontal play and hold enormous potential to scale over the long term.

- **Established internet players** need to leverage their strong B2C position and make a more aggressive move into the B2B space.

- **Specialized startups** should carve out their sweet spot for highly targeted IoT offerings—ideally in a segment that will not be better served by larger competitors.

- **Industrial and technology companies** must extend their product offerings to defend their large B2B customer base and find new ways to engage with customers across the product life cycle.

- **Telcos** can leverage their telecommunications assets and capabilities—including data access—to push beyond connectivity and provide higher-value offerings.

IoT offers tremendous opportunity, and hundreds of companies have already made big bets in this space. But it's not simple to provide the end-to-end IoT solutions that customers want and need. It is not easy for a hardware manufacturer of connected devices, for example, to acquire (or become) a software provider that delivers value in the applications and analytics layer. Moving up and down the technology stack will be a challenge.

But there is good news: companies need not simply grit their teeth and build these capabilities through hiring or M&A. They can pick the areas in which they want to compete and develop partnerships with other companies in order to build a powerful suite of end-to-end offerings. With a clear vision of where—and by whom—dollars are actually being spent in IoT, companies have a timely opportunity to gain significant traction in the IoT space, and they can position themselves to stake a claim in one of the biggest market opportunities of our generation.

Nicolas Hunke *is a partner and managing director in the Munich office of The Boston Consulting Group. You may contact him by e-mail at hunke.nicolas@bcg.com.*

Zia Yusuf *is a partner and managing director in the firm's San Francisco office. You may contact him by e-mail at yusuf.zia@bcg.com.*

Michael Rüßmann *is a senior partner and managing director in BCG's Munich office. You may contact him by e-mail at ruessmann.michael@bcg.com.*

Florian Schmieg *is a principal in the firm's Munich office. You may contact him by e-mail at schmieg.florian@bcg.com.*

Akash Bhatia *is a principal in BCG's San Francisco office. You may contact him by e-mail at bhatia.akash@bcg.com.*

Nipun Kalra *is a principal in the firm's Mumbai office. You may contact him by e-mail at kalra.nipun@bcg.com.*

LEANER, FASTER, AND BETTER WITH DEVOPS

by Hanno Ketterer and Christian N. Schmid

AGILE METHODOLOGIES HAVE GIVEN companies just what they need in the digital era: a collaborative and flexible way to develop software. (See "The End of Two-Speed IT," BCG article, August 2016.) Cross-functional teams, iterative development, and continual testing and feedback are powerful practices that have enabled companies to improve their development process. But businesses can realize even greater transformative change—and success—by implementing a second set of practices known as DevOps.

DevOps calls for some staff from IT operations, which traditionally works apart from developers, to be brought onto cross-functional agile teams. In addition, DevOps puts heavy emphasis on automation. This set of practices is not an alternative to agile but a complement—one that takes agile a step further and applies it to the rest of the software life cycle: deployment, release, operation, and monitoring.

Indeed, the results are eye opening. By implementing DevOps, the financial services company Nationwide achieved a 70% reduction in system downtime and a 50% improvement in code quality. In our experience, DevOps has helped companies tackle security issues in half the time they traditionally required, release new code on demand instead of on a fixed schedule, and reduce IT costs significantly. Indeed, companies that have combined DevOps with a standardized and fully virtualized infrastructure have seen IT costs drop by as much as 25%. Such results translate into a crucial benefit: sustainable competitive advantage.

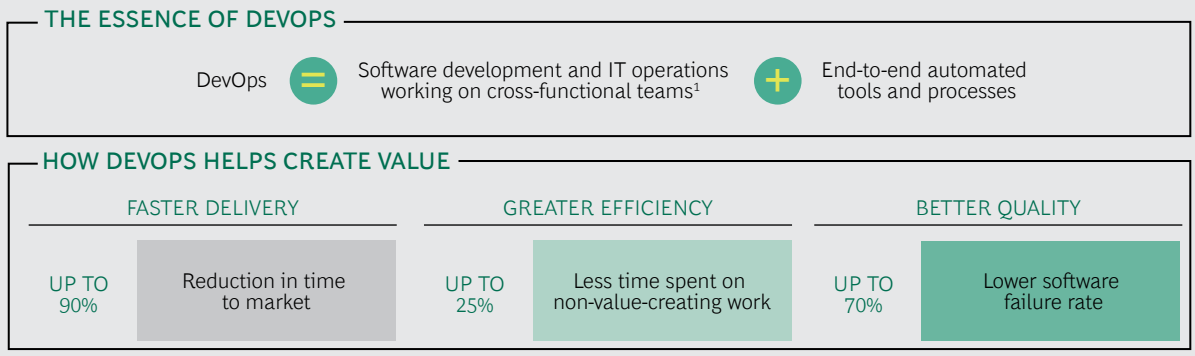
DevOps Helps Create Value

For all the benefits that agile brings, it doesn't change the basic relationship between development teams and IT operations. As a result, some companies are finding that delays persist at critical handovers because IT operations is still working in time-tested but largely manual ways. ING Bank's CIO, Ron van Kemenade, put it this way: "We found that working in an agile way solely in development didn't really make much of a difference. IT operations needed to be included as well, since that's basically where the buck stops before you go into production." (See "Building a Cutting-Edge Banking IT Function: An Interview with Ron van Kemenade, the CIO of ING Bank," BCG article, December 2015.) By bringing some staff from IT operations onto cross-functional agile teams and stressing automation, DevOps helps companies address this issue while delivering other key benefits. Indeed, DevOps creates tremendous value in three important ways. (See Exhibit 1.)

Faster Delivery of Features and Changes.

Developers—even agile ones—typically call

Exhibit 1 | DevOps Helps Improve Agility, Efficiency, and Quality



Sources: *2016 State of DevOps Report*, Puppet and DevOps Research and Assessment, 2016; *The Total Economic Impact of the Microsoft DevOps Solution*, Forrester Research, 2016; BCG analysis.
[1]Cross-functional teams typically include representatives from the business side of the company.

IT operations when they are ready to send software to testing. If the software is brand new, operations needs to configure the test environment. If the software is a new release of a current product and a test environment already exists, interfaces and side applications still need to be configured and added. These tasks, like many in operations, are labor-intensive, and a developer can deploy code only so often under such a system. Therefore, developers tend to work with large chunks of code. But this approach comes at a price: an individual change isn't released until all the revisions packed with it are working.

DevOps helps companies accelerate the time-consuming tasks in IT operations. For example, automating testing provides developers with faster feedback, and automating integration incorporates developers' changes more quickly into the code base. Such changes encourage developers to work with smaller chunks of code—even just a few lines. Then, instead of eventually releasing a big kitchen-sink application, companies can release a series of small, incremental updates, getting new features into the field fast.

Being able to release on demand is particularly beneficial when it comes to security. In "zero day" exploits, hackers try to take advantage of a vulnerability before it can be fixed. ("Zero day" refers to the fact that the software's creator effectively has zero days to solve the problem.) If creating patches follows the traditional development, testing, and release processes, the hackers' window of opportunity stays open. DevOps helps companies release fixes as needed and seal breaches fast—often within hours rather than days.

With DevOps, IT professionals can devote more time to value-creating work.

Greater Efficiency. DevOps helps IT professionals devote more time to value-creating work. For example, when companies automate testing and integration, developers no longer spend big chunks of their day waiting for machines to be configured or code to be integrated. They can do both by clicking a button on a self-service portal. After a large European bank implemented DevOps, it reported efficiency improvements of up to 25% in developing updates for its online banking application. The IT operations staff is also freed up for more challenging work that adds more value, which will prove rewarding for employee and employer alike.

Better Quality Code and Faster Recovery from Failures. After software is released, developers typically move on to their next project. Therefore, they don't have an incentive to anticipate or prevent longer-term

problems. Future fixes will be operations' headache.

DevOps keeps developers involved and on the hook throughout the life cycle of a feature or an application, resulting in better-quality code. Fewer fixes are required because developers look for and eliminate potential problems as they write code. When failures do occur, bugs are more easily traced to their source because developers are working with smaller chunks of code. Meanwhile, human error is reduced by all the automation that DevOps brings to the software life cycle. As a result, companies can deliver fixes fast.

Of course, having the right talent is critical if organizations are going to develop better-quality code. The top IT professionals embrace new approaches that deliver better results. By implementing DevOps, companies can not only attract but also retain top-tier talent. There is no better way for businesses to show that IT is on the cutting edge than by using innovative tools and methodologies.

Making DevOps Work

Like agile, DevOps has no textbook implementation model. But successful companies follow five best practices.

Automate the software life cycle in stages.

One can't overstate the importance of automation to an effective implementation of DevOps. Automation is crucial to developing quality software faster and more efficiently. But companies should see automating the software life cycle as a journey—one that should be carefully orchestrated.

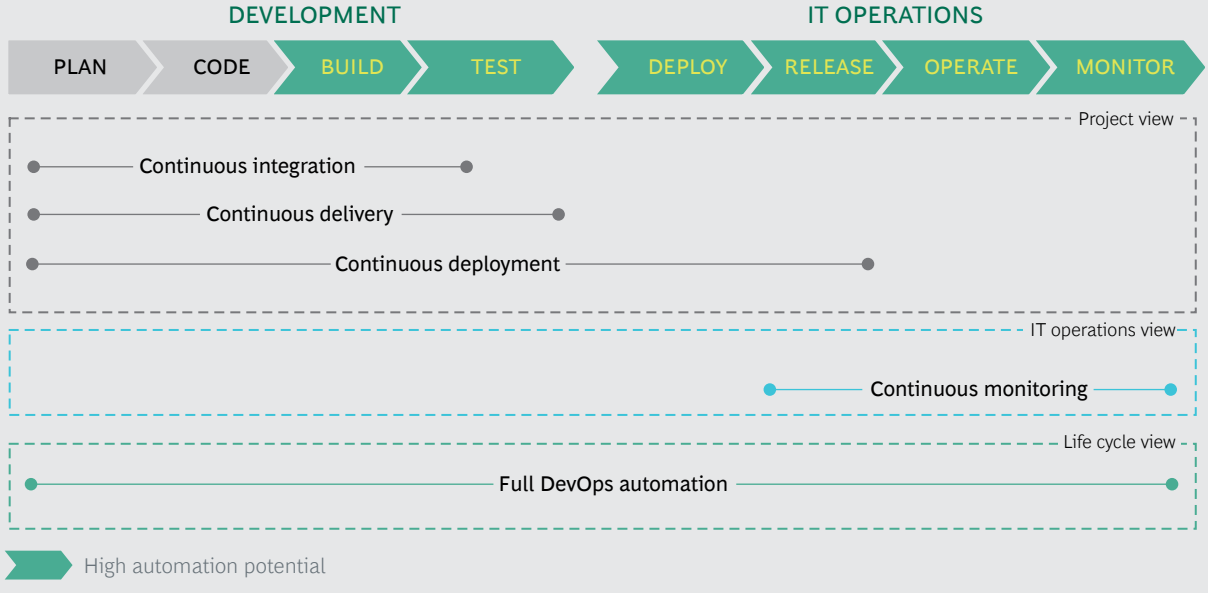
The full software life cycle encompasses many steps; which steps should be automated and in what sequence needs to be considered. For instance, automating integration testing won't eliminate bottlenecks if acceptance testing is still performed manually.

The key is to think about orchestration from the very start of a DevOps implementation. Analyze the current development process and challenge frequently used routines. If there are tests that code always passes, maybe they should be discarded rather than automated.

Companies generally implement automation in four stages (see Exhibit 2):

- **Continuous Integration.** This first step calls for software developers to merge their code with the larger code base frequently, often many times a day. Each

Exhibit 2 | DevOps Stresses Automating the Software Life Cycle



Source: BCG analysis.

time a chunk of code is integrated, the code base is automatically tested.

- **Continuous Delivery.** This is usually the next logical step. It calls for developers to work on code in cycles that are short enough for a company to reliably release an incremental update at any time. Continuous delivery doesn't mean that every change is released; sometimes changes are held back for business reasons or regulatory requirements. But there is always an update that could be released.

- **Continuous Deployment.** This stage calls for automatically deploying every change to production as long as the code has passed all testing. Not every company will want to implement this. Continuous deployment works best for businesses that need to move particularly fast in getting out new features, applications, or security measures. Online retailers and media companies are two prime examples. But companies in other industries, such as the automated investment services firm Wealthfront, have also become big proponents and beneficiaries of continuous deployment.

- **Continuous Monitoring.** Most companies will want to implement this stage, which calls for constantly assessing the behavior of released applications. It lets companies home in on—and even predict—issues as quickly as possible so that they can be prevented or corrected before they become big problems.

Standardize tools, processes, and practices. Another best practice for implementing DevOps is standardizing tools, processes, and practices across teams. This is something that is often absent within organizations. Standardized approaches, as opposed to ad hoc solutions, reduce errors and improve knowledge sharing. They are also a prerequisite for implementing automation, which lies at the heart of DevOps. For instance, automating server configuration through a self-service portal requires a defined set of configurations, instead of an endless array of possible permutations.

Standardization also reduces the overall number of tools companies use, increasing efficiency and potentially reducing costs. Traditionally, tools haven't been coordinated across IT. Developer teams and operations teams all select and manage their own tools despite any overlap. By contrast, DevOps requires an integrated, centrally managed tool chain. Companies will have to make changes, but the effort is easily outweighed by the benefits.

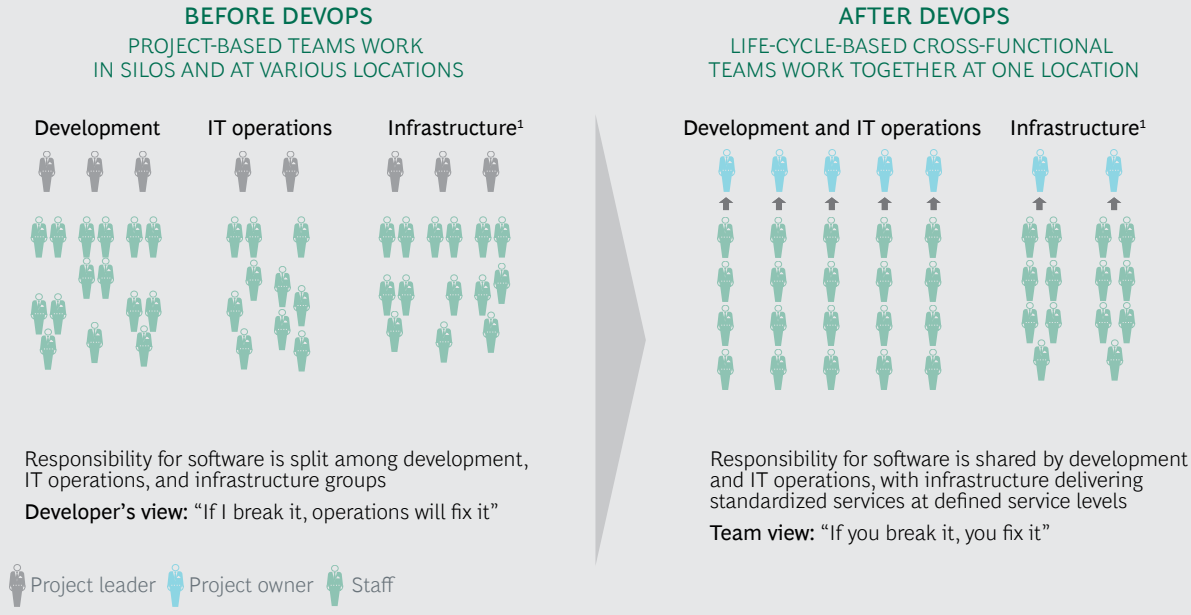
Standardized approaches are a prerequisite for automation, which lies at the heart of DevOps.

As part of their drive toward standardization, companies should challenge tradition and ask if existing tools, processes, and practices should be updated or improved. For example, we find that DevOps works particularly well in Infrastructure as a Service and Platform as a Service environments, because the necessary IT resources are available on demand. Companies that adopt these services could eliminate the need for potentially lengthy infrastructure-provisioning processes. Indeed, DevOps helps companies get the most out of cloud-based services (especially when those services are accessed through a public cloud). The cloud's ability to rapidly deploy virtual machines—and hence a company's software—is of value only if new features and changes are developed and released quickly.

On the application side, decoupled architectures—made possible by the use of standard application programming interfaces (APIs) and microservices—enable developers to build modular components. Perhaps the most important benefit to this approach is that if a faulty piece of code is deployed, only that piece—and not the whole system—fails.

Rethink the team structure. DevOps, by definition, brings the development and operations sides of IT together on cross-functional teams that have end-to-end responsibility for the full software life cycle.

Exhibit 3 | DevOps Stresses End-to-End Responsibility



Source: BCG analysis.
[1]Managing infrastructure is never the responsibility of development, IT operations, or DevOps teams.

(See Exhibit 3.) But the spirit of DevOps is about collaboration and communication among everyone with a stake in the software. So a team's roster doesn't have to end with IT; it can include other stakeholders, such as security experts. Indeed, some companies, such as Capital One, implement a variant called DevOpsSec.

As companies build their teams, they should keep several points in mind. Implementing DevOps changes the skills that employees will need. Operations personnel, for example, will no longer configure environments manually; instead they will need to write scripts that automate configuration. Determining the right team size is also critical. Although it may be tempting to include as many stakeholders as possible, large teams can make communication unwieldy. What's the best size? Generally, a team should have seven to nine members. Indeed, at Amazon, the rule of thumb is the "two-pizza team"—one that can be fed with two pizzas. Finally, depending on a company's needs, some IT professionals, such as application architects and database engineers, may be better positioned in centers of excellence than on DevOps teams. (It's important to note that DevOps teams never manage the infrastructure. That role falls to either an in-house infrastructure group or an outside provider, such as Amazon Web Services.)

Facilitate the needed cultural shift. Implementing DevOps requires cultural change, so top management must be strongly committed to the effort. Moving to agile wasn't seamless for many companies. Many of the coordinating tasks that mid-level managers had traditionally handled ceased to exist, and the managers moved onto the teams, acting more as coaches than supervisors. Pushback wasn't unusual, and it should be expected as employees from IT operations join cross-functional teams. Education, enablement, and ongoing experience with DevOps can smooth the transition, but so, too, can support from the top.

A cultural shift will be needed at the team level as well. With code changes integrated and released much more frequently, teams need to rethink, and even overturn, long-standing practices—formal and informal ones alike. Gary Gruver, former Hewlett-Packard director of engineering for LaserJet enterprise firmware, once described the dos and don'ts that the company established after it implemented continuous integration: "We had certain rules.

[If] you commit code and then you go home before it goes green, that's a lab felony."

Diplomacy may also be required. Some companies have found that bringing IT operations staff onto cross-functional teams can create certain tensions, as the employees are likely to have preexisting, and even unflattering, views of each other. One way to overcome such friction is to emphasize—and specifically, show—the value of working in this manner. Pilots that are staffed with those most open to DevOps can create champions and achieve results that promote collaboration and defuse tensions. However, finding a pilot that produces quick and clear results can be tricky. Developing a product or service that doesn't depend on a fixed release schedule—and that can be rolled out separately from other applications—is ideal.

Finally, implementing DevOps means that teams need to learn to share knowledge. Regularly having internal "DevOps days" can provide a venue for team members to spread the word about best practices while learning more about one another's roles. New hires, meanwhile, should be trained from the outset in DevOps. This will not only make their transition to a team smoother but also send a message: this is a company that is embracing new ways, and new hires can be part of the change from day one.

Develop new KPIs. As DevOps helps companies reengineer the way teams work, management should develop new KPIs to gauge how teams are performing and how processes are working. These could measure, for example, the number of code commitments occurring each day and the time between commitment and deployment to production. To home in on red flags, companies could track metrics such as the number of code commitments made each weekend or how often someone is called for help outside working hours. A solid set of KPIs helps identify not only bottlenecks but also processes that can be improved. And this highlights a crucial point: DevOps can and should evolve over time.

For today's companies, the pressure to reduce the time to market, improve efficiency, and boost quality is constantly increasing. Each day seems to bring new urgency. Agile methodologies go a long way toward helping companies develop software in the digital era; DevOps practices help them transform the software life cycle. With careful attention and planning—and management's commitment to working in the new ways that today's business landscape requires—DevOps can help companies deliver great software more efficiently and more effectively than ever before.

Hanno Ketterer *is a senior partner and managing director in the Amsterdam office of The Boston Consulting Group and the global leader of the insurance sector in the firm's Technology Advantage practice. For more than 20 years, Ketterer has led large-scale technology transformations and postmerger integrations in the banking and insurance industries. You may contact him by e-mail at ketterer.hanno@bcg.com.*

Christian N. Schmid *is a principal in BCG's Munich office. He is active in the firm's Technology Advantage practice, where he is a global leader of the DevOps topic, and he is the global segment leader of the Simplify IT topic in the Financial Institutions practice. For the past ten years, Schmid has driven large-scale transformations—including digital and agile transformations, simplification and restructuring programs, and postmerger integrations—for numerous companies. You may contact him by e-mail at schmid.c@bcg.com.*

BUILDING A CYBERRESILIENT ORGANIZATION

by Stefan A. Deutscher, Walter Bohmayr, and Alex Asen

Despite steadily mounting evidence to the contrary, many executives seem to imagine that, in the realm of cybersecurity, a robust defense is all their company needs. But those executives may experience a rude awakening. No defense, no matter how well constructed and maintained, is 100% impenetrable. Computer systems are subject to compromise. Data, including both sensitive company information and information about customers and clients, is vulnerable to theft or tampering.

The upshot: companies can't afford to focus their security efforts solely on their ability to ward off attacks and expect this strategy to fully protect them. Instead, they must ramp up their organization's *resilience*—its ability to continue to function after the company suffers a breach (as it almost inevitably will) and to recover gracefully after even a serious security lapse.

Building organizational cyberresilience entails understanding the three phases of a successful attack: the before, the during, and the after. How well your company—meaning both its own people and external parties and partners such as temporary staff and contractors—grasps and is prepared for each phase can make an enormous difference in whether a breach proves relatively innocuous or takes a massive toll on your business. (See the sidebar "Getting the People Part Right.")

Before an Attack

The period before an attack can last as long as the attacker chooses. During this phase, the attacker scouts its prey (your company) to understand its technical defenses and identify its vulnerabilities. For defenders, this is the time to take three critical steps.

Create awareness among both IT and nontechnical staff of the potential for cyberattacks. Simple yet powerful ways to raise awareness include distributing mail and video messages from top management, reporting attacks or incidents on the company's intranet site(s), and—emulating a best practice of businesses in the mining, construction, and engineering industries—making "safety moments" a mandatory part of every company meeting.

The company should supplement its ongoing awareness campaign with appropriate training. It is critical that your IT staff be able to recognize early signs of an attack, distinguish an attack from unexpected but legitimate behavior on the part of the company's IT systems, and react effectively. You should strive to create a culture that tolerates false positives—IT staff should not have to worry about crying wolf too often.

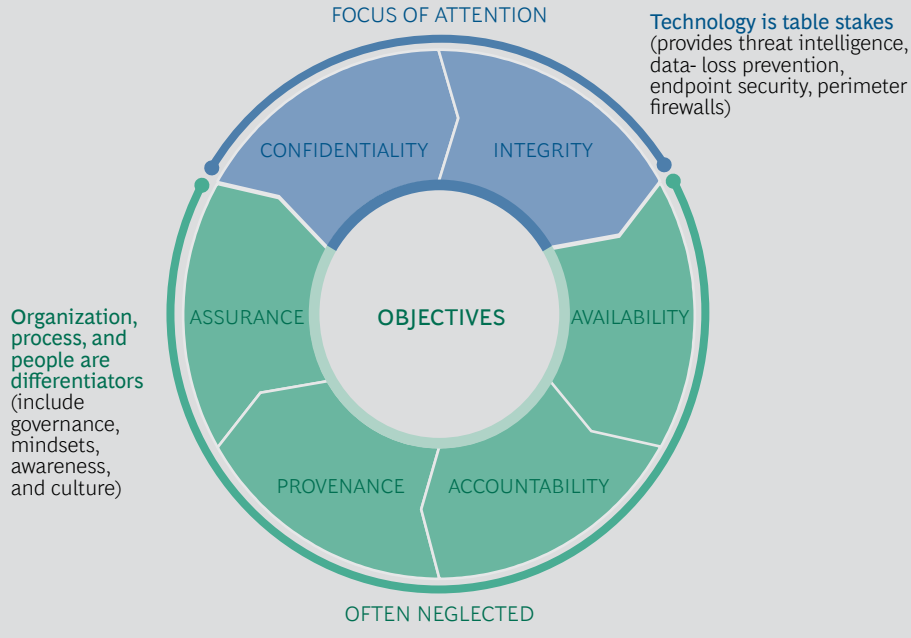
You should also ensure that nontechnical staff understand the importance of being prudent—for example, not clicking on unexpect-

GETTING THE PEOPLE PART RIGHT

A full treatment of corporate cybersecurity would span a number of topics not addressed in this article, including governance and processes. We have chosen to focus primarily on one element: the people side.

Why? Because cybersecurity starts with people. Many companies pay lip service to the importance of a holistic "people-process-technology" approach to cybersecurity. But in our experience, they tend to focus primarily on technology, while neglecting issues of organization, process, and people. (See Exhibit 1.) This can be a costly mistake, because the importance and vulnerability of people, in particular, cannot be overstated.

EXHIBIT 1 | Companies Focus Too Much on Technology and Too Little on Organization, Process, and People



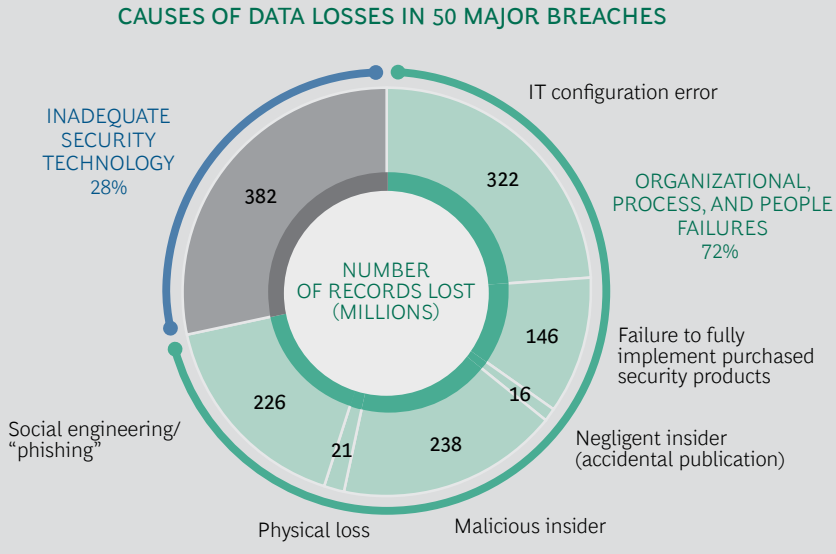
Source: BCG analysis.

ed e-mail attachments. Such prudence is vital, as today's cyberattackers are both aggressive and devious. Over the past couple of years, for example, attackers have increasingly targeted senior executives' assistants with "spear phishing" attacks (which rely on individualized, often highly tailored e-mail messages spiked with malicious attachments). A successful attack of this type can be as valuable to the attacker as one that gains direct access to the accounts of senior executives themselves, since many executive assistants have full access or far-reaching delegate rights to their bosses' mailboxes, calendars, documents, and contacts (which can be helpful to an attacker seeking to build the next step in a targeted attack).

The company should also stress the importance of such prudence to technical staff, whom attackers often target with similar tactical assaults. Administrators of pivotal IT systems (such as central infrastructure services, essential business systems, and the company's communications infrastructure) are especially popular targets of carefully designed social-engineering attacks, as well as of attacks on their private personal computers by outsiders seeking entry into the company's systems.

A company's people are crucial to establishing a successful cybersecurity program and building the resilience needed to bounce back from a breach. They will be at the forefront of designing, testing, implementing, and operating your defenses. If your people are smart, committed, well trained, and prepared, they will be your strongest bulwark against a truly damaging attack. Conversely, their failures, whether due to malicious intent, negligence, or ignorance, will likely be the source of your next breach. Indeed, a review of 50 of the largest recent data breaches reported worldwide between May 2011 and May 2016 reveals that a relatively small proportion of records lost as a result of those breaches stemmed from inadequate security technology. Most losses are attributable to failures involving organization, process, and people. (See Exhibit 2.)

Exhibit 2 | Organizational, Process, and People Failures Are the Main Source of Critical Breaches



Sources: Press reports; company statements; BCG analysis.
Note: Of the more than 1.8 billion records lost in these 50 data breaches, 490 million were excluded from our analysis because there was insufficient information to determine a root cause.

Employees throughout the organization should receive tailored training—and the training effort should start at the very top, with the organization's C-suite, board of directors, and even supervisory boards.[1] Those individuals can benefit tremendously from awareness and enablement sessions, tabletop simulation exercises, and full-fledged war-gaming sessions.[2] For technical people, the training should include special skills training—for example, lessons in how to harden systems, detect systems that do not conform to policies, and write realistic policies. For general staff, social-engineering awareness training can be very useful, especially when combined with real-life testing (using company-commissioned fake phishing e-mail messages, for example).

Think carefully about the design, implementation, and configuration of your company's technology system—especially access rights. Ensure that it covers the basics. Confirm that your technical staff have configured IT systems securely and have hardened them against attack to the extent possible.

Aim for a reasonable role-based access management system for nontechnical staff—one that keeps people separated from applica-

tions or data they don't need. (The use of expiration periods to limit access for people in specific roles is one effective way to restrain "privilege creep.") The same approach should apply to IT staff, confining their reach to systems that they need unfettered access to, ensuring that they do not claim higher-than-necessary privileges (for example, system administrator rights) for routine tasks, and enforcing appropriate logging for activities that do require higher privileges.

In the period before an attack, companies can act under their own control.

It may help to look at the practices of government entities, which commonly vet staff and assign them different security and access classifications, with different levels of permission to use certain systems. Such fine-grained control may not be economically feasible for all organizations, but studying approaches that involve this degree of sophistication can provide valuable insight into how a company might establish roles and rights in a simpler security design.

Plan for during and after while you still can.

In the period before an attack, companies can act under their own control. But when a serious attack is underway, they may be reduced to reacting or, in a worst-case scenario, simply watching as the attack unfolds. The operators of the Ukrainian power grid found themselves in precisely this state when attackers hacked the grid in December 2015.[3]

Beforehand, companies can focus on taking steps to prepare for an attack and its aftermath. These measures include what we call the "cybersecurity 101s," which include identifying the company's most valuable assets, identifying risks, defining protection objectives, and instituting appropriate risk management approaches. (See "Cybersecurity Meets IT Risk Management: A Corporate Immune and Defense System," BCG article, September 2014.) Other actions that companies can take include the following:

- Identify external parties that the company will need to engage in the event of an attack or breach, and determine how to reach them. At the same time, gauge the extent to which an internal security function can provide the desired capabilities for protection, detection, and response and whether sourcing all or part of that function might be a viable alternative.
- Write, implement, and test emergency operations, business continuity measures, and disaster recovery plans.
- Run tests and establish a testing regimen to ensure continual reassessment of the company's degree of readiness. Such testing might include tabletop simulation exercises for senior management (for example, "What would we do if our manufacturing operation in Asia was brought down by a cyberattack?") and penetration tests performed by "ethical hackers" whom the company pays to relentlessly probe and detect weaknesses in the company's defenses.
- Determine how the organization can ensure reliable, trustworthy governance during a breach, when elements of systems—including key communications such as e-mail and IP-based telephony—may be compromised or operators locked out of their systems altogether, as happened to Ukraine's grid operators when cyberattackers breached their system. (Companies may face even more serious threats during a cyberattack. During the highly publicized Carbanak attack of 2015, which targeted a large number of banks and reportedly resulted in an aggregate loss of about $1 billion, attackers could read company communications, view company videoconferences, and watch employees through their laptop cameras.)
- Create and test communications policies and plans (such as who is authorized to say what during an attack) so that the company's dissemination of information stays ahead of media coverage.
- Make sure that everyone assigned a role in emergency plans is aware of and

accepts that role. In our casework, we have found instances where named response managers had never heard of the company's emergency plan or had long since left the company. Also, make sure that every individual assigned a role has an identified backup—not just during the regular workweek, but on weekends, public holidays, and individuals' vacation days.

During an Attack

Often a company fails to recognize initially (or at all, in some instances) that an attack is unfolding—even though it has developed strong internal technical and human defense capabilities or has engaged specialized companies to provide monitoring and detection services. If and when your company sees that it is under siege, there are several important things it can do in response.

If overmatched during an attack, a company should "call in the troops."

Mobilize in a controlled way. Kick off a (prepared and practiced) standard response process. If a severe attack or breach occurs, mobilize a core response team.

Communicate to the organization that an attack is underway and that teamwork is essential. A serious attack will impose extraordinary demands on the company and its people. Providing transparency and focusing on solutions rather than on finger-pointing is important: the company and its components (organizational units, legal entities, and functions), including IT, the cybersecurity unit, HR, risk management, communications, and the business lines, must mobilize quickly and work together as a well-oiled, flexible unit to defend itself. During this period, decisions about external communication—especially on the question of how much detail to divulge—should take into account both legal concerns about revealing too much information and the potential harm to the company's brand of failing to share critical information with customers and other stakeholders in a timely manner.

Thoroughly address serious attacks, detected breaches, and loopholes as they arise. The company's various units will have to work hand in hand to ensure that people immediately report detected breaches and security loopholes to the appropriate internal parties, who must then act swiftly to mitigate the damage (or at a minimum, gain a fuller understanding of what the attack has done or is doing). Throughout the crisis, the company must also ensure that it actively manages communications with internal and external stakeholders—including employees, senior management, customers, the media, and regulators—and that it continues to meet its regulatory-reporting duties and deadlines.

Leverage external resources as necessary. Even the best-prepared organizations can find themselves overmatched during an attack. In such cases, the company should "call in the troops," which might include specialized private-sector companies and public law enforcement, as needed. The company's ability to quickly access these resources rests on preestablished contracts with the necessary parties, appropriate and well-documented processes for invoking their support, and people within the company who are authorized to kick the process into gear. Playbooks developed for the "before" period should address and document all of these needs.

After an Attack

Once the dust has settled, the company needs to ensure that it will not fall victim to the same attack a second time. (See the sidebar "'After' Is in the Eye of the Beholder.") Companies can do four things to maximize their chances of success in this effort.

Work across functions and units to understand the attack and ensure that staff have plugged the holes and updated defenses and processes. An analysis that strengthens the company's defenses and yields significant

"AFTER" IS IN THE EYE OF THE BEHOLDER

The period after an attack can mean different things to different people. For a defender, the connotation is straightforward: the immediate assault has ended, and the time to repair and regroup begins. For an attacker, however, "after" may refer to the period between the piercing of the defender's hull and the point at which the target company detects and closes the breach. Attackers use this period to exfiltrate information or to install additional malicious payload (so-called back doors or even more-advanced threats that, like sleeper cells, lie dormant and evade detection until activated from the outside).

In some instances, attackers may simply wait through much of the period between breach and detection before pulling the trigger on the poison they introduced through the breach.

In other words, sometimes the worst of the damage occurs in the "after" period. The case of Nortel (now defunct) makes this amply evident. The company believed that the attack was over, but it was actually in the middle of a breach that lasted for about ten years, in the course of which hackers had ready access to company communications and intellectual property.

lessons is much easier to conduct in an open environment, in which employees are unafraid to speak up. To foster this type of environment, organizations should institute a "blameless" postmortem culture. Such a culture has been highly effective following accidents and near-misses in the aviation industry, for example, and can facilitate learning in the aftermath of a corporate cyberbreach as well. If a culture of this type is difficult to create within the organization in a given time frame, the company should, at a minimum, establish a channel for anonymous whistleblowing—one that serves a function similar to that of an ombudsperson.

Organizations should institute a "blameless" postmortem culture.

Identify employees who can collaborate with internal and external experts on security-related issues, and establish dedicated roles for them within the company. The company may need to consult forensic companies, communications firms, training firms, auditors, legal advisors, the media, and law enforcement personnel. Once you have identified employees who can collaborate effectively with such experts, give them the latitude to concentrate on this role as necessary. Doing so may entail temporarily relieving them of their standard duties and changing reporting lines. It may also require the creation of new, dedicated positions staffed with appropriate personnel (in terms of skills and numbers).

Inform everyone affected by the attack or involved in the defense effort—including internal and external parties—that things are back to normal. This announcement will help everyone achieve closure. Here, as elsewhere, the communications department should take the lead in the company's communications efforts—but the entire organization, from top to bottom, needs to be able to communicate effectively and consistently on this front. This is also a good opportunity to thank those involved in the defense and recovery efforts (including corporate teams, individuals, and external partners, to the extent that they can be named), either before a broader audience or privately. (Not all cyberheroes will want to be publicly exposed.)

Remain vigilant. After the organization has returned to normal following a breach, it is important to combat complacency. Be sure to see the root cause analysis of the breach through to its resolution and to incorporate the knowledge gained from the experience into the company's processes, knowledge management systems, technical landscape, testing scenarios, and organizational setup.

Things to Do Monday Morning

If you are concerned about your company's ability to weather an attack or a breach, where should you focus your attention first? The following steps are very important:

- If you are starting fresh and have no data on attacks or breaches suffered by your company, review and begin to undertake the activities described above in the section "Before an Attack." If you do have such data, try to supplement it with additional threat intelligence for your industry or company. (In many instances, you can obtain this type of information from membership-based organizations and professional security services firms.)
- Run a cybersecurity health check that assesses not only the security controls that the company has in place but also the capability maturity of your organization and its processes. (See "Getting Fit for Transformation: The Other Technology Strategy Every IT Leader Needs," BCG article, July 2015.)
- Perform a training session on C-suite enablement, possibly in association with a tabletop simulation or a more detailed war-gaming exercise.
- Confirm that your company's training and corporate communications agenda includes cybersecurity-related offerings. In addition, confirm that your corporate communications department has cybersecurity-related scripts for external and internal use.
- Check that your company has developed up-to-date response plans, and verify the details of your company's contracts with outside support on call.
- Start to build a cybersecurity management system, or launch a review of your existing one.

NOTES

1. See "Why should we care about cyber resilience? Because $445 billion is at stake," World Economic Forum, September 8, 2016.
2. See "How to prepare for the cyberattack that is coming to your company," World Economic Forum, November 30, 2016.
3. See "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired,* March 3, 2016.

Stefan A. Deutscher *is an associate director in the Berlin office of The Boston Consulting Group and a core member of the Technology Advantage and Technology, Media & Telecommunications practices. He is BCG's global topic leader for cybersecurity and IT risk management as well as for IT infrastructure and data center operations. You may contact him by e-mail at deutscher.stefan@bcg.com.*

Walter Bohmayr *is a senior partner and managing director in the firm's Vienna office and a member of the Technology Advantage, Energy, Financial Institutions, and Technology, Media & Telecommunications practices. He is BCG's global leader for cybersecurity and IT risk management. You may contact him by e-mail at bohmayr.walter@bcg.com.*

Alex Asen *is a senior knowledge analyst in BCG's Boston office. He is a core member of the firm's Technology Advantage practice and a member of the global cybersecurity leadership team. You may contact him by e-mail at asen.alex@bcg.com.*

VIEWPOINT

REPORT FROM DAVOS

BOARD OVERSIGHT OF CYBERRESILIENCE

Cyberattacks, cyberbreaches, cybercrime. These are not new problems, and they are universally acknowledged to be costly, pervasive, and increasingly sophisticated. Each week, new breaches become public, most recently an incident at a large internet service provider that had gone unnoticed for more than two years. The best defense against such intrusions is cyberresilience—building in both the capability to protect yourself and your business from cyberthreats and the ability to rebound from attacks, should they happen.

Cyberresilience is a major strategy issue, and the need for boards and senior executives to give it serious attention cannot be overstated. In many industries, cyberresilience can be a source of competitive advantage, a factor for valuation in M&A situations, and a key enabler of flexible, interconnected value chains. Because it helps determine the speed at which organizations can benefit from technology innovation, it impacts value creation. But what is required to build cyberresilience, and how can boards and executives accelerate the process?

Cyberresilience cannot be left exclusively to the technology domain. Recent BCG research indicates that more than 70% of breaches exploit nontechnical vulnerabilities. For example, an attack may trick users into disclosing their legitimate credentials. The lesson here is that cyberresilience in an organization must extend beyond the technical IT domain to the domains of people, culture, and processes. A company's protective strategies and practices should apply to everything the company does—to every process on every level and across departments, units, and borders—in order to foster an appropriately security-conscious culture. Ultimate responsibility for cyberresilience rests squarely on the shoulders of boards and senior executives. It is up to them to push this culture change through the layers of their company.

In the technology domain, a division of duties and reporting lines within the organization is necessary to separate the IT implementation role (which often falls to the CIO), the IT security role (which usually falls to the CISO), and the risk management role (which tends to be the CRO's responsibility). In many cases, implementing this organizational change requires a board-level push.

> Cyberresilience cannot be left exclusively to the technology domain.

Defending against cybercrime is a new challenge for many boards. Regularly including the topic of cyberresilience on the board's agenda is especially important in such cases because the board's level of awareness of the issue is relatively low. Boards must devote considerable effort and attention to the task of supervising the transition to a new, cyberresilient state.

Boards should focus on increasing their knowledge of the topic and their level of comfort in dealing with it.

First and foremost, to challenge their executive teams on the subject of cyberresilience, they need to arm themselves with a set of principles or good practices for dealing with the issue. Multiple general recommendations exist on how to act.

BCG recently had the opportunity to support the World Economic Forum by creating a set of guidelines, designed for board-level use, that address these challenges. The Forum and its cross-industry working group have identified ten principles and backed them up with pragmatic tools to enable boards to institute them. (See the sidebar.)

The principles emphasize taking responsibility, becoming informed on the subject of cyberthreats, anchoring responsibility in the organization, and implementing plans for cyberresilience. Boards also need to join their executive team in a discussion of risk appetite, in order to define the current risk posture of their organization.

In addition, boards need tools for understanding, assessing, and quantifying the risk patterns that their organization faces today and may face in the future. A good first step is to identify the organization's most important informational assets and to determine the biggest risks to these assets. A second step is to determine how the executive team aims to manage these risks and how much its plan will cost the company. The Forum's publication includes recommendations, in the form of a Board Cyber Risk Framework, for analyzing and understanding cyberrisk at the board level.

TEN BOARD PRINCIPLES

Responsibility for Cyberresilience. The board as a whole takes ultimate responsibility for oversight of cyberrisk and cyberresilience. The board may delegate primary oversight activity to an existing committee (for example, a risk committee) or a new committee (a cyberresilience committee).

Command of the Subject. Board members receive a cyberresilience orientation upon joining the board and are regularly updated on recent threats and trends—with advice and assistance from independent external experts available as requested.

Accountable Officer. The board ensures that one corporate officer is accountable for reporting on the organization's capability to manage cyberresilience and progress in implementing cyberresilience goals. The board ensures that this officer has regular board access, sufficient authority, command of the subject matter, experience, and resources to fulfill these duties.

Integration of Cyberresilience. The board ensures that management integrates cyberresilience and cyberrisk assessment into overall business strategy and into enterprise-wide risk management, as well as budgeting and resource allocation.

Risk Appetite. The board annually defines and quantifies business risk tolerance relative to cyberresilience and ensures that this is consistent with corporate strategy and risk appetite. The board is advised on both current and future risk exposure as well as regulatory requirements and industry/societal benchmarks for risk appetite.

Risk Assessment and Reporting. The board holds management accountable for reporting a quantified and understandable assessment of cyberrisks, threats, and events as a standing agenda item during board meetings. It validates these assessments with its own strategic risk assessment using the Board Cyber Risk Framework.

Cyberresilience Plans. The board ensures that management supports the officer accountable for cyberresilience by the creation, implementation, testing, and ongoing improvement of cyberresilience plans, which are appropriately harmonized across the business. It requires the officer in charge to monitor performance and to regularly report to the board.

Community. The board encourages management to collaborate with other stakeholders, as relevant and appropriate, in order to ensure systemic cyberresilience.

Review. The board ensures that a formal, independent cyberresilience review of the organization is carried out annually.

Effectiveness. The board periodically reviews its own performance in the implementation of these principles or seeks independent advice for continuous improvement.

Emerging technologies create great changes and great opportunities, but they also expose companies to grave new risks. Examples of disruptive technologies are big data, the Internet of Things, and autonomous vehicles. Boards need to understand how disruptive technologies change their cyberrisk exposure. The Forum's publication provides insights directed toward board-level stakeholders regarding challenges such as vendor management, technology life cycle security, and the ability to quickly adapt to change.

Although cyberresilience and cyberrisk management are still young disciplines in many organizations, they are gaining speed. Boards are in a unique position to support and accelerate their development—be it to derisk their organizations' value creation or to make the world a bit safer for business partners and consumers. It is imperative that boards possess the tools necessary to increase their own understanding, to ask the right questions, and overall to develop cyberresilience.

The report by the World Economic Forum, The Boston Consulting Group, and Hewlett Packard Enterprise is available for download:

Walter Bohmayr *is a senior partner and managing director in the Vienna office of The Boston Consulting Group and a member of the Technology Advantage, Energy, Financial Institutions, and Technology, Media & Telecommunications practices. He is BCG's global leader for cybersecurity and IT risk management. You may contact him by e-mail at bohmayr.walter@bcg.com.*

Alexander Tuerk *is a project leader in the firm's Berlin office. He is a member of the Technology Advantage and Technology, Media & Telecommunications practices. You may contact him by e-mail at Tuerk.alexander@bcg.com.*

NOTE TO THE READER

Acknowledgments

The authors thank their BCG colleagues who contributed to the articles in this edition of *BCG Technology Advantage* through many discussions and comments: Ralf Dreischmeier, Philipp Englisch, Yashraj Erande, Philip Evans, David Fortune, Bernhard Georgii, Christian Haakonsen, Charles Hendren, Helge Hofmeister, Ashish Iyer, Maurice Jansen, Mark Kistulinec, Andre Lorman, Pierre Ménard, Massimo Portincaso, Martin Reeves, James Spanjaard, Sebastian Steinhäuser, Gary Wang, Sherry Wu, and Leonid Zhukov. They also thank Jürgen Schmidhuber, the codirector of the Dalle Molle Institute for Artificial Intelligence Research, and César Hidalgo, an associate professor at the Massachusetts Institute of Technology and the head of the macro connections group at the MIT Media Lab, for stimulating interactions.

They thank Astrid Blumstengel and Stuart Scantlebury for their contributions to this publication and Katherine Andrews, Gary Callahan, Alan Cohen, Catherine Cuddihee, Angela DiBattista, Pete Engardio, Kim Friedman, Abby Garland, Gerry Hill, Sara Strassenreiter, Amy Strong, and Mark Voorhees for their help in writing, editing, design, and production.

For Further Contact

Ralf Dreischmeier
Senior Partner and Managing Director
Global Leader, Technology Advantage practice
BCG London
+44 20 7753 5353
dreischmeier.ralf@bcg.com

Alex Asen
Senior Knowledge Analyst
BCG Boston
1 617 973 1200
asen.alex@bcg.com

Akash Bhatia
Principal
BCG San Francisco
+1 415 732 8000
bhatia.akash@bcg.com

Walter Bohmayr
Senior Partner and Managing Director
BCG Vienna
+43 1 537 56 80
bohmayr.walter@bcg.com

Guillaume Combastet
Principal
BCG Paris
+33 1 40 17 10 10
combastet.guillaume@bcg.com

Claude Czechowski
Senior Advisor
czechowski.claude@advisor.bcg.com

Stefan A. Deutscher
Associate Director
BCG Berlin
+49 30 28 87 10
deutscher.stefan@bcg.com

Philipp Gerbert
Senior Partner and Managing Director
BCG Munich
+49 89 23 17 40
gerbert.philipp@bcg.com

Antoine Gourevitch
Senior Partner and Managing Director
BCG Paris
+33 1 40 17 10 10
gourevitch.antoine@bcg.com

Martin Hecker
Senior Partner and Managing Director
BCG Cologne
+49 221 55 00 50
hecker.martin@bcg.com

Nicolas Hunke
Partner and Managing Director
BCG Munich
+49 89 231 740
hunke.nicolas@bcg.com

Jan Justus
Principal
BCG Munich
+49 89 231 740
justus.jan@bcg.com

Nipun Kalra
Principal
BCG Mumbai
+91 22 6749 7000
kalra.nipun@bcg.com

Hanno Ketterer
Senior Partner and Managing Director
BCG Amsterdam
+31 20 548 4000
ketterer.hanno@bcg.com

Michael Rüßmann
Senior Partner and Managing Director
BCG Munich
+49 89 231 740
ruessmann.michael@bcg.com

Christian N. Schmid
Principal
BCG Munich
+49 89 231 740
schmid.c@bcg.com

Florian Schmieg
Principal
BCG Munich
+49 89 231 740
schmieg.florian@bcg.com

Alexander Türk
Project Leader
BCG Berlin
+49 30 28 87 10
tuerk.alexander@bcg.com

Zia Yusuf
Partner and Managing Director
BCG San Francisco
+1 415 732 8000
yusuf.zia@bcg.com

To find the latest BCG content and register to receive e-alerts on this topic or others, please visit bcgperspectives.com.

Follow bcg.perspectives on Facebook and Twitter.

4/17

BCG

THE BOSTON CONSULTING GROUP

Abu Dhabi
Amsterdam
Athens
Atlanta
Auckland
Bangkok
Barcelona
Beijing
Berlin
Bogotá
Boston
Brussels
Budapest
Buenos Aires
Calgary
Canberra
Casablanca
Chennai
Chicago
Cologne
Copenhagen
Dallas
Denver
Detroit
Dubai
Düsseldorf
Frankfurt
Geneva
Hamburg
Helsinki
Ho Chi Minh City
Hong Kong
Houston
Istanbul
Jakarta
Johannesburg
Kiev
Kuala Lumpur
Lagos
Lima
Lisbon
London
Los Angeles
Luanda
Madrid
Melbourne
Mexico City
Miami
Milan
Minneapolis
Monterrey
Montréal
Moscow
Mumbai
Munich
Nagoya
New Delhi
New Jersey
New York
Oslo
Paris
Perth
Philadelphia
Prague
Rio de Janeiro
Riyadh
Rome
San Francisco
Santiago
São Paulo
Seattle
Seoul
Shanghai
Singapore
Stockholm
Stuttgart
Sydney
Taipei
Tel Aviv
Tokyo
Toronto
Vienna
Warsaw
Washington
Zurich